Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 31 Οκτωβρίου 2022
(OR. en)

14128/22

Διοργανικός φάκελος:
2022/0085(COD)

CYBER 343
TELECOM 428
INST 396
CSC 472
CSCI 157
INF 176
FIN 1158
BUDGET 22
DATAPROTECT 294
CODEC 1617

ΣΗΜΕΙΩΜΑ ΣΗΜΕΙΟΥ «I/A»

Αποστολέας:	Γενική Γραμματεία του Συμβουλίου
Αποδέκτης:	Επιτροπή των Μονίμων Αντιπροσώπων (2ο Τμήμα) / Συμβούλιο
αριθ. προηγ. εγγρ.:	10097/5/22 REV 5
Αριθ. εγγρ. Επιτρ.:	7474/22 + ADD 1
Θέμα:	Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον καθορισμό μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης — Γενική προσέγγιση

ΕΙΣΑΓΩΓΗ

1. Στις 22 Μαρτίου 2022 η Επιτροπή ενέκρινε πρόταση κανονισμού για τον καθορισμό μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης. Η πρόταση αποτελούσε ένα από τα μέτρα που προβλέπονται στη στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία[1], η οποία αποσκοπεί στην ενίσχυση της συλλογικής ανθεκτικότητας της Ένωσης έναντι των κυβερνοαπειλών.

[1] 14133/20.

Στα συμπεράσματα της 22ας Μαρτίου 2021 σχετικά με τη στρατηγική αυτή[2], το Συμβούλιο τόνισε ότι η κυβερνοασφάλεια «είναι ζωτικής σημασίας για τη λειτουργία της δημόσιας διοίκησης και των θεσμών τόσο σε εθνικό όσο και σε ενωσιακό επίπεδο, καθώς και για την κοινωνία και την οικονομία μας στο σύνολό της».

2. Η πρόταση της Επιτροπής, η οποία βασίζεται στο άρθρο 298 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, αποσκοπεί στη βελτίωση του επιπέδου κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης με τη θέσπιση κοινού πλαισίου, λαμβάνοντας δεόντως υπόψη την αυτονομία κάθε οντότητας της Ένωσης. Ειδικότερα, οι στόχοι της πρότασης είναι οι εξής:

   – ενίσχυση της εντολής και της χρηματοδότησης της ομάδας CERT-EE (αυτόνομη διοργανική ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τις οντότητες της ΕΕ)·

   – δημιουργία διοργανικής δομής (διοργανικό συμβούλιο κυβερνοασφάλειας – IICB) στην οποία θα συμμετέχουν εκπρόσωποι όλων των οντοτήτων της Ένωσης προκειμένου να εξασφαλιστεί η ορθή εφαρμογή του κανονισμού·

   – θέσπιση υποχρέωσης των ενωσιακών οντοτήτων να ανταλλάσσουν με την CERT-EE (μη διαβαθμισμένες) πληροφορίες σχετικά με περιστατικά και να κοινοποιούν σημαντικές απειλές, τρωτότητες και περιστατικά· και

   – προώθηση του συντονισμού και της συνεργασίας για την αντιμετώπιση σημαντικών περιστατικών.

3. Το Ευρωπαϊκό Κοινοβούλιο διόρισε την κα Henna Virkkunen (EPP) εισηγήτρια της αρμόδιας επιτροπής ITRE. Το σχέδιο έκθεσης εκδόθηκε στις 7 Οκτωβρίου 2022.

4. Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων γνωμοδότησε στις 17 Μαΐου 2022[3].

---

[2] 6722/21.
[3] 9252/22.

5. Στο Συμβούλιο, η εξέταση της πρότασης στο πλαίσιο της Οριζόντιας Ομάδας «Θέματα κυβερνοχώρου» (HWPCI) ξεκίνησε κατά τη διάρκεια της γαλλικής Προεδρίας, στις 29 Μαρτίου 2022. Η γαλλική Προεδρία εκπόνησε το πρώτο συμβιβαστικό κείμενο, το οποίο συζητήθηκε στο πλαίσιο της HWPCI τον Ιούνιο του 2022, και υπέβαλε έκθεση προόδου[4] στο Συμβούλιο στις 21 Ιουνίου 2022.

6. Κατά τη διάρκεια της τσεχικής Προεδρίας, η HWPCI πραγματοποίησε οκτώ ειδικές συνεδριάσεις[5] προκειμένου να συζητηθούν η πρόταση και διάφορα διαδοχικά συμβιβαστικά κείμενα.

7. Στις 23 Μαΐου 2022 η Προεδρία ζήτησε τη γνώμη της Επιτροπής Ασφαλείας του Συμβουλίου (CSC) σχετικά με τις πτυχές της πρότασης που αφορούν την ασφάλεια των πληροφοριών και ιδίως τις διαβαθμισμένες πληροφορίες. Η Επιτροπή Ασφαλείας εξέδωσε τη γνώμη της στις 19 Σεπτεμβρίου 2022[6]. Όπως ανέφερε η Επιτροπή Ασφαλείας, οι διαβαθμισμένες πληροφορίες της ΕΕ έχουν εξαιρεθεί ρητά από το πεδίο εφαρμογής του κανονισμού. Οι διατάξεις σχετικά με τις εξαιρέσεις από τις υποχρεώσεις κοινοποίησης και αναφοράς περιστατικών σχετικά με πληροφορίες που δεν προέρχονται από οντότητες της Ένωσης έχουν τροποποιηθεί αναλόγως.

8. Στις 28 Οκτωβρίου 2022 η HWPCI κατέληξε σε συμφωνία επί του συμβιβαστικού κειμένου της Προεδρίας ως έχει στο παράρτημα.

---

4 9719/22.

5 6 και 20 Ιουλίου, 13, 21 και 28 Σεπτεμβρίου, 5, 19 και 28 Οκτωβρίου 2022.

6 12603/22 + COR 1.

ΚΥΡΙΟΤΕΡΑ ΖΗΤΗΜΑΤΑ

9. Τα κράτη μέλη υποδέχθηκαν με ικανοποίηση την πρόταση εκτιμώντας ότι υποβάλλεται την κατάλληλη στιγμή και είναι συμπληρωματική προς τη μελλοντική οδηγία σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση (στο εξής: οδηγία NIS 2), τάχθηκαν δε υπέρ των γενικών της στόχων. Ωστόσο, τα κράτη μέλη ζήτησαν περαιτέρω ευθυγράμμιση με το την οδηγία NIS 2, περισσότερη αμοιβαιότητα στην ανταλλαγή πληροφοριών μεταξύ των οντοτήτων της Ένωσης και των κρατών μελών, και επισήμαναν τον υπερβολικά προαιρετικό χαρακτήρα ορισμένων από τα προτεινόμενα μέτρα. Τα κράτη μέλη δήλωσαν επίσης ότι θα προτιμούσαν να απαλειφθούν οι αναφορές στην Κοινή Μονάδα Κυβερνοχώρου, της οποίας η εντολή και η σύνθεση δεν έχουν ακόμη καθοριστεί.

10. Με βάση τις συζητήσεις στην HWPCI, τα ακόλουθα σημεία εντοπίστηκαν ως τα κύρια πολιτικά ζητήματα:

α. Ευθυγράμμιση με τη μελλοντική οδηγία NIS 2

Όπως ζητήθηκε από τα κράτη μέλη, έχουν γίνει περαιτέρω ευθυγραμμίσεις με τη μελλοντική οδηγία NIS 2, μεταξύ άλλων:

- ορισμένοι ορισμοί (άρθρο 3) έχουν ευθυγραμμιστεί με εκείνους της οδηγίας NIS 2·
- προστέθηκε νέο άρθρο 7α σχετικά με τις αξιολογήσεις από ομοτίμους σε εθελοντική βάση, σύμφωνα με την οδηγία NIS 2, προσαρμοσμένο στις ανάγκες των οντοτήτων της Ένωσης·
- οι υποχρεώσεις αναφοράς περιστατικών (άρθρο 20) έχουν ευθυγραμμιστεί με εκείνες της οδηγίας NIS 2.

β. Σύνθεση του διοργανικού συμβουλίου κυβερνοασφάλειας (IICB) (άρθρο 9)

Μετά από συζητήσεις σχετικά με την κατάλληλη συμμετοχή των εκπροσώπων των κρατών μελών στις εργασίες του IICB, επιτεύχθηκε συμβιβασμός μέσω δήλωσης του Συμβουλίου προς καταχώριση στα πρακτικά.

γ. Θεσμική αυτονομία

Επιτεύχθηκε μια ισορροπημένη προσέγγιση ανάμεσα στη βούληση των κρατών μελών να ενισχύσουν τους μηχανισμούς συμμόρφωσης και στην ανάγκη σεβασμού της αρχής της θεσμικής αυτονομίας, ιδίως όσον αφορά τους ελέγχους και τα πειθαρχικά μέτρα (άρθρο 11).

Τέλος, η αναφορά σε συγκεκριμένο ποσοστό του προϋπολογισμού ΤΠ που διατίθεται στην κυβερνοασφάλεια απαλείφθηκε από την αιτιολογική σκέψη 8.

ΣΥΜΠΕΡΑΣΜΑ

11. Η Επιτροπή των Μόνιμων Αντιπροσώπων καλείται:

(α) να εγκρίνει το συμβιβαστικό κείμενο ως έχει στο παράρτημα, το οποίο στη συνέχεια θα αποτελέσει την εντολή για διαπραγματεύσεις με το Ευρωπαϊκό Κοινοβούλιο,

(β) να εισηγηθεί στο Συμβούλιο να εγκρίνει το συμβιβαστικό κείμενο ως έχει στο παράρτημα κατά τη σύνοδό του στις 18 Νοεμβρίου 2022 και να καταχωρίσει στα πρακτικά τη δήλωση του Συμβουλίου ως έχει στην προσθήκη του παρόντος εγγράφου.

ΠΑΡΑΡΤΗΜΑ

2022/0085 (COD)

Πρόταση

ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

για τον καθορισμό μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 298,

Έχοντας υπόψη τη Συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας Ατομικής Ενεργείας και ιδίως το άρθρο 106α,

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία,

Εκτιμώντας τα ακόλουθα:

(1) Στην ψηφιακή εποχή, η τεχνολογία των πληροφοριών και των επικοινωνιών αποτελεί ακρογωνιαίο λίθο για μια ανοικτή, αποτελεσματική και ανεξάρτητη ενωσιακή διοίκηση. Η εξελισσόμενη τεχνολογία και η αυξημένη πολυπλοκότητα και διασυνδεσιμότητα των ψηφιακών συστημάτων επιτείνουν τους κινδύνους κυβερνοασφάλειας, καθιστώντας την ενωσιακή διοίκηση περισσότερο ευάλωτη σε κυβερνοαπειλές και σχετικά περιστατικά, στοιχείο που εντέλει απειλεί την επιχειρησιακή συνέχεια της διοίκησης και την ικανότητά της να προστατεύει τα δεδομένα της. Παρότι η αυξημένη χρήση των υπηρεσιών υπολογιστικού νέφους, η γενικευμένη χρήση της τεχνολογίας των πληροφοριών, ο υψηλός βαθμός ψηφιοποίησης, η τηλεργασία και η εξελισσόμενη τεχνολογία και συνδεσιμότητα αποτελούν σήμερα βασικά χαρακτηριστικά όλων των δραστηριοτήτων των διοικητικών οντοτήτων της Ένωσης, η ψηφιακή ανθεκτικότητα δεν έχει ακόμη αναπτυχθεί επαρκώς.

(2) Το τοπίο των κυβερνοαπειλών που αντιμετωπίζουν οι […] **οντότητες** της Ένωσης εξελίσσεται συνεχώς. Οι τακτικές, οι τεχνικές και οι διαδικασίες που χρησιμοποιούν οι παράγοντες απειλής εξελίσσονται συνεχώς, ενώ τα κύρια κίνητρα τέτοιων επιθέσεων μεταβάλλονται ελάχιστα, από την κλοπή πολύτιμων πληροφοριών που δεν έχουν δημοσιοποιηθεί έως τον προσπορισμό χρημάτων, τη χειραγώγηση της κοινής γνώμης ή την υπονόμευση των ψηφιακών υποδομών. Ο ρυθμός με τον οποίο πραγματοποιούν τις κυβερνοεπιθέσεις τους αυξάνεται συνεχώς, ενώ οι εκστρατείες τους γίνονται ολοένα και πιο εξελιγμένες και αυτοματοποιημένες, στρεφόμενες κατά διαρκώς επεκτεινόμενων επιφανειών εκτεθειμένων σε επιθέσεις και εκμεταλλευόμενες γρήγορα τις τρωτότητες.

(3) Τα περιβάλλοντα ΤΠ των […] **οντοτήτων** της Ένωσης έχουν αλληλεξαρτήσεις και ενοποιημένες ροές δεδομένων, ενώ οι χρήστες τους συνεργάζονται στενά. Λόγω της διασύνδεσης αυτής, οποιαδήποτε διαταραχή, ακόμη και όταν αρχικά περιορίζεται σε συγκεκριμέν[…]**η οντότητα** της Ένωσης, μπορεί να επιφέρει ευρύτερα αλυσιδωτά αποτελέσματα και να έχει ενδεχομένως ως αποτέλεσμα εκτεταμένες και μακροχρόνιες αρνητικές επιπτώσεις σε άλλες οντότητες. Επιπλέον, τα περιβάλλοντα ΤΠ ορισμένων […] **οντοτήτων της Ένωσης** συνδέονται με τα περιβάλλοντα ΤΠ των κρατών μελών, με αποτέλεσμα ένα περιστατικό που επηρεάζει μία οντότητα της Ένωσης να ενέχει κίνδυνο για την κυβερνοασφάλεια των περιβαλλόντων ΤΠ των κρατών μελών και αντίστροφα. **Επιπλέον, οι οντότητες της Ένωσης χειρίζονται μεγάλο όγκο συχνά ευαίσθητων πληροφοριών από τα κράτη μέλη και, ως εκ τούτου, τα περιστατικά θα μπορούσαν επίσης να επηρεάσουν αρνητικά τα κράτη μέλη. Για τον λόγο αυτό, η κυβερνοασφάλεια των οντοτήτων της Ένωσης έχει μεγάλη σημασία και για τα κράτη μέλη**. **Πληροφορίες σχετικά με συγκεκριμένα περιστατικά μπορούν επίσης να διευκολύνουν τον εντοπισμό παρόμοιων κυβερνοαπειλών ή περιστατικών που επηρεάζουν τα κράτη μέλη.**

(4) **Οι οντότητες**[…] της Ένωσης αποτελούν ελκυστικούς στόχους και έρχονται αντιμέτωπες με παράγοντες απειλής οι οποίοι διαθέτουν υψηλή ειδίκευση και επάρκεια πόρων, καθώς και με άλλες απειλές. Ταυτόχρονα, το επίπεδο και η ωριμότητα της κυβερνοανθεκτικότητας, καθώς και η ικανότητα εντοπισμού και αντιμετώπισης κακόβουλων δραστηριοτήτων στον κυβερνοχώρο ποικίλλουν σημαντικά μεταξύ αυτών των οντοτήτων. Ως εκ τούτου, είναι αναγκαίο για τη λειτουργία της ευρωπαϊκής διοίκησης […] **οι οντότητες** της Ένωσης να επιτύχουν υψηλό κοινό επίπεδο κυβερνοασφάλειας μέσω **της εφαρμογής μέτρων κυβερνοασφάλειας,** […] καθώς και μέσω της ανταλλαγής πληροφοριών και της συνεργασίας.

(5) Η οδηγία [πρόταση οδηγίας NIS 2] σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση αποσκοπεί στην περαιτέρω βελτίωση των ικανοτήτων ανθεκτικότητας και αντιμετώπισης περιστατικών στον τομέα της κυβερνοασφάλειας των δημόσιων και ιδιωτικών οντοτήτων, των εθνικών αρμόδιων αρχών και φορέων, καθώς και της Ένωσης στο σύνολό της. Επομένως, **οι οντότητες** […] της Ένωσης είναι ανάγκη να ακολουθήσουν παρόμοια πορεία θεσπίζοντας κανόνες που συμφωνούν με την οδηγία [πρόταση οδηγίας NIS 2] και αντικατοπτρίζουν το επίπεδο φιλοδοξίας της.

(6) Για να επιτευχθεί υψηλό κοινό επίπεδο κυβερνοασφάλειας, είναι αναγκαίο […] **κάθε οντότητα** της Ένωσης να θεσπίσει εσωτερικό πλαίσιο διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας, το οποίο να διασφαλίζει την αποτελεσματική και συνετή διαχείριση όλων των κινδύνων κυβερνοασφάλειας […]. **Το πλαίσιο θα πρέπει να καθορίζει πολιτικές κυβερνοασφάλειας, συμπεριλαμβανομένων διαδικασιών για την αξιολόγηση της αποτελεσματικότητας των ήδη εφαρμοζόμενων μέτρων κυβερνοασφάλειας. Το πλαίσιο θα πρέπει να βασίζεται σε μια προσέγγιση για όλους τους κινδύνους, η οποία αποσκοπεί στην προστασία των δικτυακών και πληροφοριακών συστημάτων και των υποδομών των εν λόγω συστημάτων από συμβάντα όπως κλοπές, πυρκαγιές, πλημμύρες, διακοπές στις τηλεπικοινωνίες ή την παροχή ρεύματος, ή μη εξουσιοδοτημένη φυσική πρόσβαση και ζημία, καθώς και παρεμβολές στις εγκαταστάσεις παροχής και επεξεργασίας πληροφοριών οντότητας της Ένωσης, που θα μπορούσαν να υπονομεύσουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων που αποθηκεύονται, διαβιβάζονται, υποβάλλονται σε επεξεργασία ή είναι προσβάσιμα μέσω δικτυακών και πληροφοριακών συστημάτων. Στο πλαίσιο θα πρέπει να αποτυπώνονται τα πορίσματα της ανάλυσης κινδύνου, λαμβάνοντας υπόψη όλους τους σχετικούς τεχνικούς, επιχειρησιακούς και οργανωτικούς κινδύνους για την κυβερνοασφάλεια της οικείας οντότητας της Ένωσης.**

(6α) Για τη διαχείριση των κινδύνων που εντοπίζονται βάσει του πλαισίου, κάθε οντότητα της Ένωσης θα πρέπει να διασφαλίζει τη λήψη κατάλληλων και αναλογικών τεχνικών, επιχειρησιακών και οργανωτικών μέτρων. Τα μέτρα αυτά θα πρέπει να καλύπτουν τους τομείς, συμπεριλαμβανομένων των μέτρων κυβερνοασφάλειας, που ορίζονται στον παρόντα κανονισμό για την ενίσχυση της κυβερνοασφάλειας κάθε οντότητας της Ένωσης.

(6β) Τα περιουσιακά στοιχεία και οι κίνδυνοι που προσδιορίζονται στο πλαίσιο, καθώς και τα συμπεράσματα που προκύπτουν από τακτικές αξιολογήσεις του επιπέδου ωριμότητας θα πρέπει να αντικατοπτρίζονται στο σχέδιο κυβερνοασφάλειας που καταρτίζει κάθε οντότητα της Ένωσης. Το σχέδιο κυβερνοασφάλειας θα πρέπει να περιλαμβάνει τα εγκριθέντα μέτρα κυβερνοασφάλειας, με στόχο την αύξηση της συνολικής κυβερνοασφάλειας της οικείας οντότητας της Ένωσης.

(6γ) Δεδομένου ότι η διασφάλιση της κυβερνοασφάλειας αποτελεί συνεχή διαδικασία, η καταλληλότητα και η αποτελεσματικότητα όλων των μέτρων θα πρέπει να αναθεωρούνται τακτικά υπό το πρίσμα των μεταβαλλόμενων κινδύνων, των περιουσιακών στοιχείων και του επιπέδου ωριμότητας των οντοτήτων της Ένωσης. Το πλαίσιο θα πρέπει να επανεξετάζεται τακτικά και τουλάχιστον ανά τριετία, ενώ το σχέδιο κυβερνοασφάλειας θα πρέπει να αναθεωρείται τουλάχιστον ανά διετία ή μετά από κάθε αξιολόγηση του επιπέδου ωριμότητας ή κάθε επανεξέταση του πλαισίου.

(6δ) Οι οντότητες της Ένωσης θα πρέπει να ανταλλάσσουν σχετικές πληροφορίες σε τακτική βάση, μεταξύ άλλων όσον αφορά σχετικά περιστατικά και κυβερνοαπειλές, διασφαλίζοντας παράλληλα την εμπιστευτικότητα και την κατάλληλη προστασία των πληροφοριών που παρέχει η αναφέρουσα οντότητα της Ένωσης.

(6ε) Θα πρέπει να εφαρμοστεί μηχανισμός για τη διασφάλιση της αποτελεσματικής ανταλλαγής πληροφοριών, του συντονισμού και της συνεργασίας των οντοτήτων της Ένωσης σε περίπτωση σημαντικών περιστατικών, συμπεριλαμβανομένου σαφούς προσδιορισμού των ρόλων και των αρμοδιοτήτων των εμπλεκόμενων οντοτήτων της Ένωσης. Οι πληροφορίες που ανταλλάσσονται θα πρέπει να λαμβάνονται υπόψη από το καθορισμένο σημείο επαφής για το EU-CyCLONe, κατά την ανταλλαγή σχετικών πληροφοριών με το EU-CyCLONe ως συμβολή στην κοινή αντίληψη της κατάστασης.

(7) Οι διαφορές μεταξύ των **οντοτήτων** […] της Ένωσης απαιτούν ευελιξία κατά την εφαρμογή, δεδομένου ότι δεν ταιριάζει σε όλες τις περιπτώσεις η ίδια προσέγγιση. Τα μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας δεν θα πρέπει να περιλαμβάνουν υποχρεώσεις που παρεμβαίνουν άμεσα στην άσκηση των αποστολών που έχουν ανατεθεί […] **στις οντότητες** της Ένωσης ή θίγουν τη θεσμική αυτονομία τους. Ως εκ τούτου, […] **οι εν λόγω οντότητες** θα πρέπει να θεσπίσουν τα δικά τους πλαίσια διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας **και σχέδια κυβερνοασφάλειας**, και να εγκρίνουν […] **μέτρα** κυβερνοασφάλειας. **Κατά την εφαρμογή των εν λόγω μέτρων, θα πρέπει να λαμβάνονται δεόντως υπόψη οι υφιστάμενες συνέργειες μεταξύ των οντοτήτων της Ένωσης, με σκοπό την ορθή διαχείριση των πόρων και τη βελτιστοποίηση του κόστους. Θα πρέπει επίσης να υπάρχει η δέουσα μέριμνα ώστε τα μέτρα να μην επηρεάζουν αρνητικά την αποτελεσματική ανταλλαγή πληροφοριών και τις δραστηριότητες των οντοτήτων της Ένωσης με άλλες οντότητες της Ένωσης και εθνικές αρμόδιες αρχές.**

(8) Για την αποφυγή δυσανάλογης οικονομικής και διοικητικής επιβάρυνσης των […] **οντοτήτων** της Ένωσης, οι απαιτήσεις σχετικά με τη διαχείριση κινδύνων κυβερνοασφάλειας θα πρέπει να είναι ανάλογες προς τον κίνδυνο που ενέχει το σχετικό δικτυακό και πληροφοριακό σύστημα, λαμβανομένων υπόψη των πλέον προηγμένων τεχνολογικών εξελίξεων όσον αφορά τα σχετικά μέτρα. Κάθε […] **οντότητα** της Ένωσης θα πρέπει να στοχεύει στη διάθεση επαρκούς ποσοστού του προϋπολογισμού της που αφορά την ΤΠ στη βελτίωση του επιπέδου κυβερνοασφάλειάς της. **Η αξιολόγηση του επιπέδου ωριμότητας θα πρέπει επίσης να αξιολογεί κατά πόσον οι δαπάνες της οντότητας της Ένωσης για την κυβερνοασφάλεια είναι ανάλογες προς τους κινδύνους που αντιμετωπίζει.**

(9) Για την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας, η κυβερνοασφάλεια θα πρέπει να τελεί υπό την εποπτεία του ανώτατου διοικητικού επιπέδου κάθε […] **οντότητας** της Ένωσης. […] **Το ανώτατο διοικητικό επίπεδο θα πρέπει να επιβλέπει την εφαρμογή του παρόντος κανονισμού, συμπεριλαμβανομένης της θέσπισης του πλαισίου διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας και των σχεδίων κυβερνοασφάλειας, συμπεριλαμβανομένων μέτρων κυβερνοασφάλειας**. Η δημιουργία νοοτροπίας κυβερνοασφάλειας, δηλαδή η καθημερινή πρακτική της κυβερνοασφάλειας, αποτελεί αναπόσπαστο μέρος […] **ενός πλαισίου** κυβερνοασφάλειας σε […] **όλες τις οντότητες** της Ένωσης.

(10) Τα μέτρα […] [...] **κυβερνοασφάλειας** θα πρέπει να αποτελούν μέρος […] **του σχεδίου** κυβερνοασφάλειας και να εξειδικεύονται περαιτέρω σε έγγραφα καθοδήγησης ή συστάσεις που εκδίδονται από τη CERT-ΕΕ. Κατά τον καθορισμό μέτρων και κατευθυντήριων γραμμών, θα πρέπει να λαμβάνονται δεόντως υπόψη **τα πλέον προηγμένα και, κατά περίπτωση, τα οικεία ευρωπαϊκά και διεθνή πρότυπα, καθώς και** η σχετική νομοθεσία και οι πολιτικές της ΕΕ, συμπεριλαμβανομένων των αξιολογήσεων κινδύνου και των συστάσεων που εκδίδονται από την ομάδα συνεργασίας NIS, όπως η συντονισμένη εκτίμηση κινδύνου της ΕΕ και η εργαλειοθήκη της ΕΕ για την κυβερνοασφάλεια των δικτύων πέμπτης γενιάς (5G). Επιπλέον, θα μπορούσε να απαιτείται πιστοποίηση των σχετικών προϊόντων, υπηρεσιών και διαδικασιών ΤΠΕ, στο πλαίσιο ειδικών συστημάτων πιστοποίησης της κυβερνοασφάλειας της ΕΕ που εγκρίνονται σύμφωνα με το άρθρο 49 του κανονισμού (ΕΕ) 2019/881. **Κατά περίπτωση, η CERT-ΕΕ θα πρέπει να συνεργάζεται με τον ENISA.**

(11) Τον Μάιο του 2011, οι γενικοί γραμματείς των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης αποφάσισαν να συγκροτήσουν ομάδα προδιαμόρφωσης για την ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης (CERT-EE), υπό την εποπτεία διοργανικής διοικούσας επιτροπής. Τον Ιούλιο του 2012, οι γενικοί γραμματείς επιβεβαίωσαν τις πρακτικές ρυθμίσεις και συμφώνησαν να διατηρηθεί η CERT-EE ως μόνιμη οντότητα ώστε να συνεχίσει να συμβάλλει στη βελτίωση του συνολικού επιπέδου ασφάλειας της τεχνολογίας πληροφοριών των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης ως παράδειγμα ορατής διοργανικής συνεργασίας στον τομέα της κυβερνοασφάλειας. Τον Σεπτέμβριο του 2012, η CERT-EE συστάθηκε ως ειδική ομάδα της Ευρωπαϊκής Επιτροπής με διοργανική εντολή. Τον Δεκέμβριο του 2017, τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης συνήψαν διοργανική ρύθμιση σχετικά με την οργάνωση και λειτουργία της CERT-EE[7]. **Ο παρών κανονισμός** […] θα πρέπει […] **να παράσχει ένα ολοκληρωμένο σύνολο κανόνων σχετικά με την οργάνωση, τη λειτουργία και την επιχειρησιακή λειτουργία της CERT-EE. Οι διατάξεις του παρόντος κανονισμού υπερισχύουν των διατάξεων της διοργανικής συμφωνίας για την οργάνωση και τη λειτουργία της CERT-EE που συνήφθη τον Δεκέμβριο του 2017.**

[...]

[7] ΕΕ C 12 της 13.1.2018, σ. 1.

(13) Πολλές κυβερνοεπιθέσεις αποτελούν μέρος ευρύτερων εκστρατειών που έχουν ως στόχο ομάδες […] **οντοτήτων** της Ένωσης ή κοινότητες ενδιαφέροντος που περιλαμβάνουν […] **οντότητες** της Ένωσης. Για να καταστούν δυνατά ο προδραστικός εντοπισμός, η αντιμετώπιση περιστατικών ή η εφαρμογή μέτρων μετριασμού, […] **οι οντότητες** της Ένωσης θα πρέπει να κοινοποιούν στη CERT-ΕΕ […] κυβερνοαπειλές, […] τρωτότητες**, παρ' ολίγον περιστατικά και** […] περιστατικά και να ανταλλάσσουν κατάλληλες τεχνικές λεπτομέρειες που καθιστούν δυνατό τον εντοπισμό ή τον μετριασμό παρόμοιων κυβερνοαπειλών, **τρωτοτήτων, παρ' ολίγον περιστατικών και** περιστατικών, καθώς και την αντιμετώπισή τους, σε […] **άλλες οντότητες** της Ένωσης. Ακολουθώντας την ίδια προσέγγιση με αυτήν που προβλέπεται στην οδηγία [πρόταση οδηγίας NIS 2], όταν οι οντότητες **της Ένωσης** λαμβάνουν γνώση σημαντικού περιστατικού, θα πρέπει να υποχρεούνται να υποβάλουν […] **έγκαιρη προειδοποίηση** στη CERT-ΕΕ εντός 24 ωρών. Η εν λόγω ανταλλαγή πληροφοριών θα πρέπει να παρέχει στη CERT-ΕΕ τη δυνατότητα να διαδίδει τις πληροφορίες σε […] **άλλες οντότητες** της Ένωσης, καθώς και σε κατάλληλους ομολόγους τους, ώστε να συμβάλλει στην προστασία των περιβαλλόντων ΤΠ της Ένωσης και των περιβαλλόντων ΤΠ των ομολόγων της Ένωσης από παρόμοια περιστατικά […].

(13α) Ο παρών κανονισμός θεσπίζει μια προσέγγιση πολλαπλών σταδίων ως προς την αναφορά σημαντικών περιστατικών, προκειμένου να επιτευχθεί η σωστή ισορροπία μεταξύ, αφενός, της ταχείας αναφοράς, που συμβάλλει στον μετριασμό της πιθανής εξάπλωσης σημαντικών περιστατικών και επιτρέπει στις οντότητες της Ένωσης να αναζητούν συνδρομή και, αφετέρου, της υποβολής εμπεριστατωμένων αναφορών που αντλούν πολύτιμα διδάγματα από μεμονωμένα περιστατικά και βελτιώνουν με την πάροδο του χρόνου την κυβερνοανθεκτικότητα μεμονωμένων οντοτήτων της Ένωσης. Στο πλαίσιο αυτό, ο παρών κανονισμός θα πρέπει να περιλαμβάνει την αναφορά περιστατικών τα οποία, βάσει αρχικής αξιολόγησης που διενεργείται από την οντότητα της Ένωσης, θα μπορούσαν να προκαλέσουν σοβαρή διαταραχή στην επιχειρησιακή λειτουργία της οντότητας της Ένωσης ή οικονομική ζημία στην οικεία οντότητα της Ένωσης ή να επηρεάσουν άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία. Αυτή η αρχική αξιολόγηση θα πρέπει να λαμβάνει υπόψη, μεταξύ άλλων, τα θιγόμενα δικτυακά και πληροφοριακά συστήματα, ιδίως τη σημασία τους για τη λειτουργία της οντότητας της Ένωσης, τη σοβαρότητα και τα τεχνικά χαρακτηριστικά μιας κυβερνοαπειλής και τυχόν υποκείμενες τρωτότητες που αποτελούν αντικείμενο εκμετάλλευσης, καθώς και την πείρα της οντότητας της Ένωσης από παρόμοια περιστατικά. Δείκτες όπως ο βαθμός στον οποίο θίγεται η λειτουργία της οντότητας της Ένωσης, η διάρκεια ενός περιστατικού ή ο αριθμός των θιγόμενων φυσικών ή νομικών προσώπων θα μπορούσαν να διαδραματίσουν σημαντικό ρόλο στον χαρακτηρισμό της διαταραχής στην επιχειρησιακή λειτουργία ως σοβαρής.

(13β) Καθώς οι υποδομές και τα δίκτυα της σχετικής οντότητας της Ένωσης και του κράτους μέλους στο οποίο βρίσκεται η εν λόγω οντότητα της Ένωσης είναι διασυνδεδεμένα, η χωρίς αδικαιολόγητη καθυστέρηση ενημέρωση του εν λόγω κράτους μέλους για σημαντικό περιστατικό εντός της εν λόγω οντότητας της Ένωσης είναι καίριας σημασίας. Για τον σκοπό αυτό, η θιγόμενη οντότητα της Ένωσης θα πρέπει να ενημερώνει τον εθνικό ομόλογο της CERT-EE, ο οποίος ορίζεται από το κράτος μέλος σύμφωνα με την οδηγία [πρόταση NIS 2], τηρώντας το ίδιο χρονοδιάγραμμα με αυτό που ισχύει για την αναφορά σημαντικού περιστατικού στην CERT-EE. Η CERT-EE θα πρέπει επίσης να ενημερώνει τον εν λόγω εθνικό ομόλογο όταν λαμβάνει γνώση σημαντικού περιστατικού εντός του κράτους μέλους, εκτός εάν έχει ήδη αναφερθεί από την θιγόμενη οντότητα της Ένωσης.

(14) Επιπλέον της ανάθεσης περισσότερων καθηκόντων και διευρυμένου ρόλου στη CERT-ΕΕ, θα πρέπει να δημιουργηθεί διοργανικό συμβούλιο κυβερνοασφάλειας (στο εξής: ΙΙCB), το οποίο, **προκειμένου να διευκολύνει την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας μεταξύ των οντοτήτων της Ένωσης**, θα πρέπει **να έχει αποκλειστικό ρόλο** […] […] **στην** παρακολούθηση της εφαρμογής του παρόντος κανονισμού από […] **τις οντότητες** της Ένωσης, καθώς και […]**στην** εποπτεία της υλοποίησης των γενικών προτεραιοτήτων και στόχων από τη CERT-ΕΕ και την παροχή στρατηγικών κατευθύνσεων στη CERT-ΕΕ. Το ΙΙCB θα πρέπει**, ως εκ τούτου,** να διασφαλίζει την εκπροσώπηση των θεσμικών οργάνων και να περιλαμβάνει εκπροσώπους των λοιπών οργάνων και οργανισμών μέσω του Δικτύου Οργανισμών της Ένωσης. **Η οργάνωση και η λειτουργία του ΙΙCB θα πρέπει να ρυθμίζονται περαιτέρω από τον εσωτερικό κανονισμό του, ο οποίος μπορεί να περιλαμβάνει περαιτέρω διευκρινίσεις για τις τακτικές συνεδριάσεις του ΙΙCB, συμπεριλαμβανομένων των ετήσιων συναντήσεων σε πολιτικό επίπεδο, όπου εκπρόσωποι του ανώτατου διοικητικού επιπέδου κάθε μέλους του ΙΙCB θα δίνουν τη δυνατότητα στο ΙΙCB να πραγματοποιεί στρατηγικές συζητήσεις και θα του παρέχουν στρατηγική καθοδήγηση. Επιπλέον, το ΙΙCB μπορεί να διορίσει εκτελεστική επιτροπή για να το επικουρεί στο έργο του και να της αναθέσει ορισμένα από τα καθήκοντα και τις αρμοδιότητές του, ιδίως όσον αφορά καθήκοντα που απαιτούν** […] **ειδική εμπειρογνωσία των μελών της, για παράδειγμα την έγκριση του καταλόγου υπηρεσιών και τυχόν επακόλουθων επικαιροποιήσεών του, τις λεπτομέρειες για τις συμφωνίες σε επίπεδο υπηρεσιών, τις αξιολογήσεις των εγγράφων και των εκθέσεων που υποβάλλουν οι οντότητες της Ένωσης στο ΙΙCB σύμφωνα με τον παρόντα κανονισμό ή καθήκοντα που αφορούν την προετοιμασία των αποφάσεων που εκδίδει το ΙΙCB σχετικά με μέτρα συμμόρφωσης, καθώς και την παρακολούθηση της εφαρμογής τους. Το ΙΙCB θα πρέπει να θεσπίζει τον κανονισμό της εκτελεστικής επιτροπής, συμπεριλαμβανομένων των καθηκόντων και εξουσιών της.**

(15) Η CERT-ΕΕ θα πρέπει να στηρίζει την εφαρμογή μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας μέσω προτάσεων για έγγραφα καθοδήγησης και συστάσεις προς το ΙΙCB ή μέσω της έκδοσης εκκλήσεων για ανάληψη δράσης. Τα εν λόγω έγγραφα καθοδήγησης και οι συστάσεις θα πρέπει να εγκρίνονται από το ΙΙCB. Όταν είναι απαραίτητο, η CERT-ΕΕ θα πρέπει να εκδίδει εκκλήσεις για ανάληψη δράσης στις οποίες περιγράφονται επείγοντα μέτρα ασφάλειας τα οποία καλούνται να λάβουν […] **οι οντότητες** της Ένωσης εντός καθορισμένου χρονικού πλαισίου**. Το ΙΙCB δύναται να εκδίδει εντολή προς τη CERT-ΕΕ για την έκδοση, την ανάκληση ή την τροποποίηση πρότασης για έγγραφα καθοδήγησης ή σύσταση, ή έκκληση για ανάληψη δράσης.**

(16) Το ΙΙCB θα πρέπει να παρακολουθεί τη συμμόρφωση με τον παρόντα κανονισμό, καθώς και τις εξελίξεις όσον αφορά έγγραφα καθοδήγησης και συστάσεις, και εκκλήσεις για ανάληψη δράσης […]. Το ΙΙCB θα πρέπει να υποστηρίζεται σε τεχνικά θέματα από τεχνικές συμβουλευτικές ομάδες οι οποίες θα συγκροτούνται κατά την κρίση του ΙΙCB και οι οποίες θα πρέπει να συνεργάζονται στενά με τη CERT-ΕΕ, […] **τις οντότητες** της Ένωσης και άλλα ενδιαφερόμενα μέρη, κατά περίπτωση. […] **Όταν το ΙΙCB διαπιστώσει ότι οντότητες της Ένωσης δεν έχουν εφαρμόσει ή υλοποιήσει τον παρόντα κανονισμό, περιλαμβανομένων των εγγράφων καθοδήγησης, των συστάσεων ή των εκκλήσεων για ανάληψη δράσης που έχουν εκδοθεί δυνάμει του παρόντος κανονισμού, με την επιφύλαξη των εσωτερικών διαδικασιών της οικείας οντότητας της Ένωσης, δύναται να προχωρήσει στην επιβολή μέτρων συμμόρφωσης. Ο βαθμός αυστηρότητας των μέτρων συμμόρφωσης που επιβάλλονται θα πρέπει να αυξάνεται σταδιακά, πράγμα που σημαίνει ότι, όταν το ΙΙCB εγκρίνει την επιβολή μέτρων συμμόρφωσης, θα πρέπει να ξεκινά με προειδοποίηση ως το λιγότερο αυστηρό μέτρο και, εάν είναι αναγκαίο, να κλιμακώνει τα μέτρα αυτά μέχρι το αυστηρότερο, δηλαδή την έκδοση επίσημης προειδοποίησης με την οποία συστήνεται προσωρινή αναστολή των ροών δεδομένων προς την οικεία οντότητα της Ένωσης· το εν λόγω μέτρο θα εφαρμόζεται σε εξαιρετικές περιπτώσεις μακροπρόθεσμης, εσκεμμένης και/ή σοβαρής μη συμμόρφωσης της οικείας οντότητας με την υποχρέωσή της δυνάμει του παρόντος κανονισμού.**

(16α) Η προειδοποίηση αποτελεί το λιγότερο αυστηρό μέτρο συμμόρφωσης για την αντιμετώπιση των ελλείψεων που εντοπίστηκαν στην οντότητα της Ένωσης και περιλαμβάνει συστάσεις για την τροποποίηση των εγγράφων της που αφορούν την κυβερνοασφάλεια, εντός συγκεκριμένου χρονικού πλαισίου. Η προειδοποίηση θα πρέπει να είναι διαθέσιμη σε όλες τις οντότητες της Ένωσης, εκτός εάν ο παραλήπτης περιορίζεται καταλλήλως σύμφωνα με τον παρόντα κανονισμό.

(16β) Το ΙΙCB δύναται επίσης να προβεί σε σύσταση για τη διενέργεια ελέγχου σε οντότητα της Ένωσης. Για τον σκοπό αυτό, η οντότητα της Ένωσης μπορεί να απευθυνθεί στη μονάδα εσωτερικού ελέγχου της. Το ΙΙCB θα μπορούσε επίσης να ζητήσει τη διενέργεια ελέγχου από τρίτο φορέα παροχής υπηρεσιών ελέγχου, μεταξύ άλλων από αμοιβαία αποδεκτό πάροχο υπηρεσιών του ιδιωτικού τομέα.

(16γ) Με βάση τα αποτελέσματα ελέγχου που έχει διενεργηθεί κατόπιν σύστασης ή αιτήματος του ΙΙCB, το ΙΙCB μπορεί να ζητήσει από την οντότητα της Ένωσης να ευθυγραμμίσει περαιτέρω τη διαχείριση, τη διακυβέρνηση και τον έλεγχο των κινδύνων κυβερνοασφάλειας με τις διατάξεις του παρόντος κανονισμού.

(16δ) Δεδομένου του ευαίσθητου χαρακτήρα πληροφοριών που τα κράτη μέλη ανταλλάσσουν με οικείες οντότητες της Ένωσης, η κυβερνοασφάλεια του αποδέκτη των εν λόγω πληροφοριών είναι υψίστης σημασίας για τα κράτη μέλη. Κατά συνέπεια, σε εξαιρετικές περιπτώσεις μακροπρόθεσμης, εσκεμμένης, επαναλαμβανόμενης και/ή σοβαρής μη εκπλήρωσης της υποχρέωσης της οντότητας της Ένωσης, το ΙΙCB μπορεί να απευθύνει ως έσχατη λύση επίσημη προειδοποίηση σε όλα τα κράτη μέλη και τις οντότητες της Ένωσης με την οποία συστήνει προσωρινή αναστολή των ροών δεδομένων προς την οντότητα της Ένωσης, και η οποία θα πρέπει να παραμείνει σε ισχύ έως ότου επανορθωθεί η κατάσταση της κυβερνοασφάλειας της εν λόγω οντότητας. Η επίσημη αυτή προειδοποίηση θα πρέπει να γνωστοποιείται σε όλα τα κράτη μέλη και τις οντότητες της Ένωσης μέσω κατάλληλων ασφαλών διαύλων επικοινωνίας.

(16ε) **Για να διασφαλιστεί η ορθή εφαρμογή του παρόντος κανονισμού, εφόσον το ΙΙCB θεωρεί ότι τυχόν συνεχής παραβίαση του παρόντος κανονισμού από οντότητα της Ένωσης έχει προκληθεί άμεσα από πράξεις ή παραλείψεις μέλους του προσωπικού της, συμπεριλαμβανομένου του ανώτατου διοικητικού επιπέδου, θα πρέπει να ζητεί από την οικεία οντότητα της Ένωσης να λάβει τα κατάλληλα μέτρα κατά του εν λόγω μέλους του προσωπικού, σύμφωνα με τον κανονισμό υπηρεσιακής κατάστασης, καθώς και άλλους ισοδύναμους κανόνες που ισχύουν σε ορισμένες οντότητες της Ένωσης. Τα μέτρα αυτά μπορούν να περιλαμβάνουν, για παράδειγμα, πειθαρχικές διαδικασίες και, όπου αρμόζει, στην ειδική περίπτωση των οργανισμών της Ένωσης, αίτημα προς την αρμόδια αρχή να προβεί στις απαραίτητες ενέργειες για την πιθανή απαλλαγή από τα καθήκοντά του προσώπου που ενδέχεται να ευθύνεται για τη συνεχή παράβαση του παρόντος κανονισμού.**

(17) Η CERT-ΕΕ θα πρέπει να έχει ως αποστολή να συμβάλλει στην ασφάλεια του περιβάλλοντος ΤΠ όλων των […] **οντοτήτων** της Ένωσης. **Όταν εξετάζει το ενδεχόμενο να παράσχει τεχνικές συμβουλές ή στοιχεία για συναφή ζητήματα πολιτικής κατόπιν αιτήματος οντότητας της Ένωσης, η CERT-ΕΕ θα πρέπει να βεβαιώνεται ότι αυτό δεν εμποδίζει την εκπλήρωση των άλλων καθηκόντων της που ορίζονται στον παρόντα κανονισμό.**

(17α) Η CERT-ΕΕ θα πρέπει να λειτουργεί ως το αντίστοιχο όργανο του ορισθέντος συντονιστή για […] **τις οντότητες** της Ένωσης, για τον σκοπό της συντονισμένης γνωστοποίησης τρωτοτήτων στο ευρωπαϊκό μητρώο τρωτοτήτων που αναφέρεται στο άρθρο 6 της οδηγίας [πρόταση οδηγίας NIS 2], **και θα πρέπει να αναπτύξει πολιτική για τη διαχείριση των τρωτοτήτων, συμπεριλαμβανομένης της προώθησης και διευκόλυνσης της οικειοθελούς συντονισμένης γνωστοποίησης τρωτοτήτων.**

[...]

(19) Η CERT-ΕΕ θα πρέπει επίσης να εκπληρώνει τον ρόλο που προβλέπεται στην οδηγία [πρόταση οδηγίας NIS 2] όσον αφορά τη συνεργασία και την ανταλλαγή πληροφοριών με το δίκτυο των ομάδων αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (στο εξής: CSIRT). Επιπλέον, σύμφωνα με τη σύσταση της Επιτροπής (ΕΕ) 2017/1584[8], η CERT-ΕΕ θα πρέπει να συνεργάζεται με τα σχετικά ενδιαφερόμενα μέρη και να συντονίζει από κοινού την αντιμετώπιση. Προκειμένου να συμβάλλει στην επίτευξη υψηλού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση, η CERT-ΕΕ θα πρέπει να ανταλλάσσει πληροφορίες σχετικά με συγκεκριμένα περιστατικά με τους εθνικούς ομολόγους της. Η CERT-ΕΕ θα πρέπει επίσης να συνεργάζεται με άλλους ομολόγους από τον δημόσιο και τον ιδιωτικό τομέα, μεταξύ άλλων στο επίπεδο του ΝΑΤΟ, με την επιφύλαξη προηγούμενης έγκρισης από το ΙΙCB.

[8] Σύσταση (ΕΕ) 2017/1584 της Επιτροπής, της 13ης Σεπτεμβρίου 2017, για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο (ΕΕ L 239 της 19.9.2017, σ. 36).

(20) Για τη στήριξη της επιχειρησιακής κυβερνοασφάλειας, η CERT-ΕΕ θα πρέπει να χρησιμοποιεί τη διαθέσιμη εμπειρογνωσία του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια **(ENISA)** μέσω διαρθρωμένης συνεργασίας, όπως προβλέπεται στον κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[9]. Όπου κρίνεται κατάλληλο, θα πρέπει να θεσπίζονται συγκεκριμένες ρυθμίσεις μεταξύ των δύο οντοτήτων με σκοπό τον καθορισμό της πρακτικής εφαρμογής της εν λόγω συνεργασίας και την αποφυγή της αλληλεπικάλυψης δραστηριοτήτων. Η CERT-ΕΕ θα πρέπει να συνεργάζεται με τον […] **ENISA** όσον αφορά την ανάλυση απειλών και να του κοινοποιεί την έκθεσή της για το τοπίο των απειλών σε τακτική βάση.

[...]

(22) **Οι δραστηριότητες και ο χειρισμός πληροφοριών της CERT-ΕΕ δυνάμει του παρόντος κανονισμού ενδέχεται να περιλαμβάνουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα.** Σε όλες τις περιπτώσεις στις οποίες πραγματοποιείται επεξεργασία δεδομένων προσωπικού χαρακτήρα δυνάμει του παρόντος κανονισμού, η επεξεργασία αυτή θα πρέπει να εκτελείται σύμφωνα με τη νομοθεσία για την προστασία των δεδομένων, συμπεριλαμβανομένου του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[10]. **Όταν, σύμφωνα με τον παρόντα κανονισμό, δεδομένα προσωπικού χαρακτήρα διαβιβάζονται προς εγκατεστημένους στην Ένωση αποδέκτες που δεν είναι οντότητες της Ένωσης, θα πρέπει τηρούνται οι διατάξεις του άρθρου 9 του κανονισμού (ΕΕ) 2018/1725.**

---

9 Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) (ΕΕ L 151 της 7.6.2019, σ. 15).

10 Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (ΕΕ L 295 της 21.11.2018, σ. 39).

(23) Ο χειρισμός πληροφοριών από τη CERT-ΕΕ και [...] **τις οντότητες** της Ένωσης θα πρέπει να συνάδει με τους **εφαρμοστέους** κανόνες […] για την ασφάλεια των πληροφοριών[…]. […]

(23α) Για τους σκοπούς της ανταλλαγής πληροφοριών, χρησιμοποιούνται εμφανείς σημάνσεις που υποδεικνύουν ότι οι αποδέκτες των πληροφοριών πρέπει να τηρούν ορισμένα όρια κατά την ανταλλαγή πληροφοριών βάσει, ιδίως, συμφωνιών τήρησης του απορρήτου ή άτυπων συμφωνιών τήρησης του απορρήτου, όπως το πρωτόκολλο για την ανταλλαγή πληροφοριών «traffic light» ή άλλες σαφείς ενδείξεις από την πηγή. Το πρωτόκολλο για την ανταλλαγή πληροφοριών «traffic light» πρέπει να νοείται ως μέσο ενημέρωσης για τυχόν περιορισμούς όσον αφορά την περαιτέρω διάδοση πληροφοριών. Χρησιμοποιείται σε όλες σχεδόν τις ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT) και σε ορισμένα κέντρα ανάλυσης και ανταλλαγής πληροφοριών.

(24) **Ο παρών κανονισμός και τα νέα καθήκοντα που ανατίθενται στην CERT-ΕΕ δεν θα επηρεάσουν τις συνολικές δαπάνες στο πλαίσιο του πολυετούς δημοσιονομικού πλαισίου.** Δεδομένου ότι οι υπηρεσίες και τα καθήκοντα της CERT-ΕΕ είναι προς το συμφέρον όλων των […] **οντοτήτων** της Ένωσης, κάθε […] **οντότητα** της Ένωσης με δαπάνες ΤΠ θα πρέπει να συνεισφέρει δίκαιο μερίδιο στις εν λόγω υπηρεσίες και καθήκοντα. Οι συνεισφορές αυτές δεν θίγουν τη δημοσιονομική αυτονομία των […] **οντοτήτων** της Ένωσης. **Όλες οι οντότητες της Ένωσης και οι διοικήσεις τους θα πρέπει να διασφαλίζουν τη βελτιστοποίηση των πόρων τους στο τρέχον επίπεδο και να ενισχύουν την αποτελεσματικότητα, μεταξύ άλλων με την εμβάθυνση της διοργανικής συνεργασίας στον τομέα της κυβερνοασφάλειας. Ως εκ τούτου, θα πρέπει να δοθεί προτεραιότητα σε μια κοινή προσέγγιση για τη συγκέντρωση των διοικητικών δαπανών έναντι των δαπανών των οντοτήτων της Ένωσης σε μεμονωμένη βάση.**

(25) Το IICB, με τη συνδρομή της CERT-EE, θα πρέπει να επανεξετάζει και να αξιολογεί την εφαρμογή του παρόντος κανονισμού και να υποβάλει έκθεση με τα πορίσματά του στην Επιτροπή. Με βάση αυτά τα στοιχεία, η Επιτροπή θα πρέπει να υποβάλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο, στην Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και στην Επιτροπή των Περιφερειών. **Επιπλέον, το Ευρωπαϊκό Ελεγκτικό Συνέδριο καλείται να αξιολογεί τη λειτουργία της CERT-EE σε τακτική βάση.**

ΕΞΕΔΩΣΑΝ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Κεφάλαιο I
ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1

Αντικείμενο

1. Ο παρών κανονισμός θεσπίζει **μέτρα που αποσκοπούν στην επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας εντός των οντοτήτων της Ένωσης** [...]

2. Προς τούτο, ο κανονισμός καθορίζει:

(γ) υποχρεώσεις βάσει των οποίων **κάθε** [...] **οντότητα** της Ένωσης οφείλει να θεσπίσει [...] πλαίσιο διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας·

(δ) υποχρεώσεις διαχείρισης κινδύνων κυβερνοασφάλειας, [...]**,** αναφοράς σημαντικών περιστατικών **και ανταλλαγής πληροφοριών** για **τις οντότητες** της Ένωσης·

(ε) κανόνες σχετικά με την οργάνωση, **τη λειτουργία** και την επιχειρησιακή λειτουργία της [...] **αυτόνομης διοργανικής ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική** για […] **τις οντότητες** της Ένωσης (στο εξής: CERT-EE) και σχετικά με την οργάνωση, **τη λειτουργία** και την επιχειρησιακή λειτουργία του διοργανικού συμβουλίου κυβερνοασφάλειας **(IICB)**·

(στ) κανόνες σχετικά με την παρακολούθηση της εφαρμογής του παρόντος κανονισμού.

Άρθρο 2

Πεδίο εφαρμογής

1. Ο παρών κανονισμός εφαρμόζεται σε [...] όλες τις [...] **οντότητες** της Ένωσης και στη [...] [...] CERT-ΕΕ και στο **ΠΣΒ** [...].

2. Ο παρών κανονισμός εφαρμόζεται με την επιφύλαξη της θεσμικής αυτονομίας σύμφωνα με τις Συνθήκες.

3. Με εξαίρεση το άρθρο 12 παράγραφος 7, ο παρών κανονισμός δεν εφαρμόζεται στα δικτυακά και πληροφοριακά συστήματα που χειρίζονται διαβαθμισμένες πληροφορίες της ΕΕ (στο εξής: ΔΠΕΕ).

Άρθρο 3

Ορισμοί

Για τους σκοπούς του παρόντος κανονισμού, ισχύουν οι ακόλουθοι ορισμοί:

1) «[…] **οντότητες** της Ένωσης»: τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης που έχουν ιδρυθεί με τη Συνθήκη για την Ευρωπαϊκή Ένωση, τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης ή τη Συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας, ή βάσει των Συνθηκών αυτών·

2) «δικτυακό και πληροφοριακό σύστημα»: δικτυακό και πληροφοριακό σύστημα […] **όπως ορίζεται στο** άρθρο 4 σημείο 1) της οδηγίας [πρόταση οδηγίας NIS 2]·

3) «ασφάλεια δικτυακών και πληροφοριακών συστημάτων»: ασφάλεια δικτυακών και πληροφοριακών συστημάτων […] **όπως ορίζεται στο** άρθρο 4 σημείο 2) της οδηγίας [πρόταση οδηγίας NIS 2]·

4) «κυβερνοασφάλεια»: η κυβερνοασφάλεια […] **όπως ορίζεται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 2019/881**·

5) «ανώτατο διοικητικό επίπεδο»: διοικητικό στέλεχος, όργανο διοίκησης ή συντονισμού και εποπτείας στο ανώτερο διοικητικό επίπεδο **με ικανότητες λήψης αποφάσεων**, λαμβανομένων υπόψη των ρυθμίσεων διακυβέρνησης υψηλού επιπέδου σε κάθε […] **οντότητα** της Ένωσης·

5α) «παρ' ολίγον περιστατικό»: παρ' ολίγον περιστατικό όπως ορίζεται στο άρθρο 4 σημείο 4α) της οδηγίας [πρόταση οδηγίας NIS 2]·

6) «περιστατικό»: περιστατικό […] **όπως ορίζεται στο** άρθρο 4 σημείο 5) της οδηγίας [πρόταση οδηγίας NIS 2]·

[...]

8) «σημαντικό **περιστατικό**»: κάθε περιστατικό **που προκαλεί διαταραχή η οποία υπερβαίνει την ικανότητα μιας οντότητας και της CERT-EE να ανταποκριθεί σε αυτήν ή που έχει σημαντικό αντίκτυπο σε τουλάχιστον δύο οντότητες της Ένωσης·**
[...]

9) «χειρισμός περιστατικών»: χειρισμός περιστατικών […] **όπως ορίζεται στο** άρθρο 4 σημείο 6) της οδηγίας [πρόταση οδηγίας NIS 2]·

10) «κυβερνοαπειλή»: κυβερνοαπειλή […] **όπως ορίζεται στο** άρθρο 2 σημείο 8) του κανονισμού (ΕΕ) 2019/881·

[...]

12) «τρωτότητα»: τρωτότητα κατά την έννοια του άρθρου 4 σημείο 8) της οδηγίας [πρόταση οδηγίας NIS 2]·

[...]

14) «[…] κίνδυνος»: **κίνδυνος κατά την έννοια του άρθρου 4 σημείο 7β) της οδηγίας [πρόταση οδηγίας NIS 2]**[…]·

[...]

[...]

Άρθρο 3α

Επεξεργασία δεδομένων προσωπικού χαρακτήρα

1) Η επεξεργασία δεδομένων προσωπικού χαρακτήρα δυνάμει του παρόντος κανονισμού από την CERT-EE, το IICB ή οντότητες της Ένωσης διενεργείται σύμφωνα με τον κανονισμό (ΕΕ) 2018/1725.

2) Η CERT-EE, το IICB και οι οντότητες της Ένωσης επεξεργάζονται και ανταλλάσσουν δεδομένα προσωπικού χαρακτήρα στον βαθμό που είναι αναγκαίο και με αποκλειστικό σκοπό την εκπλήρωση των αντίστοιχων υποχρεώσεών τους δυνάμει του παρόντος κανονισμού.

Κεφάλαιο ΙΙ
ΜΕΤΡΑ ΓΙΑ ΥΨΗΛΟ ΚΟΙΝΟ ΕΠΙΠΕΔΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Άρθρο 4

Πλαίσιο διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων

1. Κάθε […] **οντότητα** της Ένωσης θεσπίζει το δικό της […] πλαίσιο διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας («το πλαίσιο») προς στήριξη της αποστολής της οντότητας […]**.** […] **Το πλαίσιο** εποπτεύεται από το ανώτατο διοικητικό επίπεδο της οντότητας, ώστε να διασφαλίζεται η αποτελεσματική και συνετή διαχείριση όλων των κινδύνων κυβερνοασφάλειας. Το πλαίσιο τίθεται σε εφαρμογή το αργότερο έως …. [15 μήνες μετά την έναρξη ισχύος του παρόντος κανονισμού].

2. Το πλαίσιο καλύπτει ολόκληρο το μη διαβαθμισμένο περιβάλλον ΤΠ της οικείας […] **οντότητας της Ένωσης**, συμπεριλαμβανομένων τυχόν περιβάλλοντος ΤΠ εντός των εγκαταστάσεων, **δικτύου λειτουργικής τεχνολογίας,** περιουσιακών στοιχείων και υπηρεσιών που λειτουργούν εξωτερικά σε περιβάλλοντα νεφοϋπολογιστικής ή φιλοξενούνται από τρίτους, κινητών συσκευών, εταιρικών δικτύων, επιχειρηματικών δικτύων που δεν συνδέονται με το διαδίκτυο και τυχόν συσκευών που συνδέονται με το περιβάλλον ΤΠ. Το πλαίσιο **βασίζεται σε μια προσέγγιση για όλους τους κινδύνους και σε αξιολόγηση του επιπέδου ωριμότητας σύμφωνα με το άρθρο 6 που καλύπτει όλους τους σχετικούς τεχνικούς, λειτουργικούς και οργανωτικούς κινδύνους που θα μπορούσαν να επηρεάσουν την κυβερνοασφάλεια της οικείας οντότητας της Ένωσης** […].

2α. **Το πλαίσιο καθορίζει πολιτικές κυβερνοασφάλειας, συμπεριλαμβανομένων στόχων και προτεραιοτήτων για την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων, καθώς και πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των εφαρμοζόμενων μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας και καθορίζει τον ρόλο και τις αρμοδιότητες των μελών του προσωπικού.**

2β. Το πλαίσιο επανεξετάζεται τακτικά, και τουλάχιστον ανά τριετία, υπό το πρίσμα των μεταβαλλόμενων κινδύνων, των περιουσιακών στοιχείων και του επιπέδου ωριμότητας της οντότητας της Ένωσης.

3. Το ανώτατο διοικητικό επίπεδο κάθε […] **οντότητας** της Ένωσης **εποπτεύει** […] τη συμμόρφωση του […] **οικείου** οργάνου/οργανισμού με τις υποχρεώσεις που σχετίζονται με τη διαχείριση, τη διακυβέρνηση και τον έλεγχο κινδύνων κυβερνοασφάλειας, με την επιφύλαξη των επίσημων αρμοδιοτήτων άλλων επιπέδων διοίκησης για τη συμμόρφωση και τη διαχείριση κινδύνων στους αντίστοιχους τομείς αρμοδιότητάς τους.

3α. **Κατά περίπτωση και με την επιφύλαξη της ευθύνης του για την εφαρμογή του παρόντος κανονισμού, το ανώτατο επίπεδο διοίκησης κάθε οντότητας της Ένωσης μπορεί να αναθέτει σε άλλους ανώτερους υπαλλήλους εντός της οικείας οντότητας συγκεκριμένες υποχρεώσεις δυνάμει του παρόντος κανονισμού. Ανεξάρτητα από την πιθανή ανάθεση συγκεκριμένων υποχρεώσεών του, το ανώτατο επίπεδο διοίκησης μπορεί να θεωρηθεί υπεύθυνο για τη μη συμμόρφωση των οντοτήτων με τις υποχρεώσεις που απορρέουν από τον παρόντα κανονισμό.**

3β. Το ανώτατο επίπεδο διοίκησης κάθε οντότητας της Ένωσης διασφαλίζει ότι οι οντότητες της Ένωσης εγκρίνουν το σχέδιο κυβερνοασφάλειας που περιλαμβάνει μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας, σύμφωνα με την οικεία ανάλυση κινδύνου, ώστε το πλαίσιο να εφαρμόζεται σύμφωνα με τον παρόντα κανονισμό.

[...]

5. Κάθε […] **οντότητα** της Ένωσης διορίζει τοπικό υπεύθυνο κυβερνοασφάλειας ή άλλο πρόσωπο με αντίστοιχες ευθύνες, που ενεργεί ως ενιαίο σημείο επαφής όσον αφορά όλες τις πτυχές της κυβερνοασφάλειας.

Ο τοπικός υπεύθυνος κυβερνοασφάλειας διευκολύνει την εφαρμογή του παρόντος κανονισμού και υποβάλλει εκθέσεις απευθείας στο ανώτατο διοικητικό επίπεδο σε τακτική βάση σχετικά με την πορεία της εφαρμογής.

Χωρίς να θίγεται ο ρόλος του τοπικού υπεύθυνου κυβερνοασφάλειας ως ενιαίου σημείου επαφής σε κάθε οντότητα της Ένωσης, μια οντότητα της Ένωσης μπορεί να αναθέτει στη CERT-ΕΕ ορισμένα καθήκοντα του τοπικού υπευθύνου κυβερνοασφάλειας όσον αφορά την εφαρμογή του παρόντος κανονισμού βάσει συμφωνίας σε επίπεδο υπηρεσιών που συνάπτεται μεταξύ της εν λόγω οντότητας της Ένωσης και της CERT-ΕΕ. Το ΙΙCB αποφασίζει κατά πόσον η παροχή της υπηρεσίας αυτής αποτελεί μέρος των βασικών υπηρεσιών της CERT-ΕΕ, λαμβάνοντας υπόψη τους ανθρώπινους και οικονομικούς πόρους της οικείας οντότητας της Ένωσης. Οι διορισμένοι τοπικοί υπεύθυνοι κυβερνοασφάλειας και κάθε μεταγενέστερη αλλαγή τους κοινοποιούνται από κάθε οντότητα της Ένωσης στη CERT-ΕΕ χωρίς αδικαιολόγητη καθυστέρηση. Η CERT-ΕΕ τηρεί τακτικά επικαιροποιημένο κατάλογο των διορισμένων τοπικών υπευθύνων κυβερνοασφάλειας.

6. Τα ανώτερα διοικητικά στελέχη με την έννοια του άρθρου 29 παράγραφος 2 του κανονισμού υπηρεσιακής κατάστασης[11] ή άλλα στελέχη αντίστοιχου βαθμού από κάθε οντότητα της Ένωσης παρακολουθούν σε τακτική βάση ειδικά προγράμματα κατάρτισης, ώστε να αποκτούν επαρκείς γνώσεις και δεξιότητες προκειμένου να κατανοούν και να αξιολογούν τους κινδύνους και τις πρακτικές διαχείρισης της κυβερνοασφάλειας, καθώς και τον αντίκτυπό τους στις δραστηριότητες του οργανισμού.

---

11 Κανονισμός αριθ. 259/68 του Συμβουλίου της 29ης Φεβρουαρίου 1968 περί καθορισμού του κανονισμού υπηρεσιακής καταστάσεως των υπαλλήλων και του καθεστώτος που εφαρμόζεται επί του λοιπού προσωπικού των Ευρωπαϊκών Κοινοτήτων, ΕΕ L 56 της 4ης Μαρτίου 1968.

7. Κάθε οντότητα της Ένωσης εφαρμόζει αποτελεσματικούς μηχανισμούς για να διασφαλίζει ότι οι δαπάνες για την κυβερνοασφάλεια ανέρχονται σε επαρκές ποσοστό του προϋπολογισμού για την ΤΠ. Κατά τον καθορισμό του ποσοστού αυτού λαμβάνεται δεόντως υπόψη το πλαίσιο.

Άρθρο 5

Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας […]

1. […] **Κάθε οντότητα της Ένωσης, υπό την εποπτεία του** ανώτατου διοικητικού επιπέδου της […]**, διασφαλίζει ότι λαμβάνονται κατάλληλα και αναλογικά τεχνικά, λειτουργικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων που εντοπίζονται δυνάμει του πλαισίου που αναφέρεται στο άρθρο 4 παράγραφος 1 και για την πρόληψη και/ή την ελαχιστοποίηση του αντικτύπου των περιστατικών. Λαμβάνοντας υπόψη τις πλέον προηγμένες τεχνολογικές εξελίξεις και, κατά περίπτωση, τα σχετικά ευρωπαϊκά και διεθνή πρότυπα, καθώς και το κόστος εφαρμογής, τα εν λόγω μέτρα εξασφαλίζουν επίπεδο ασφάλειας των δικτυακών και πληροφοριακών συστημάτων αντίστοιχο των κινδύνων που τίθενται. Κατά την αξιολόγηση της αναλογικότητας των εν λόγω μέτρων, λαμβάνεται δεόντως υπόψη ο βαθμός έκθεσης της οντότητας σε κινδύνους, το μέγεθός της, η πιθανότητα εμφάνισης περιστατικών και η σοβαρότητά τους, συμπεριλαμβανομένου του κοινωνικού και οικονομικού αντικτύπου τους.**

[...]

3. Οι οντότητες της Ένωσης εξετάζουν τουλάχιστον τους ακόλουθους ειδικούς τομείς κατά την εφαρμογή των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας στο πλαίσιο των σχεδίων κυβερνοασφάλειάς τους, σύμφωνα με τα έγγραφα καθοδήγησης και τις συστάσεις του ΙΙCB:

α) πολιτική κυβερνοασφάλειας, όσον αφορά τον προσδιορισμό των εργαλείων και των μέτρων που απαιτούνται για την επίτευξη των στόχων και των προτεραιοτήτων που αναφέρονται στο άρθρο 4 και στο άρθρο 5 παράγραφος 4·

β) πολιτικές ανάλυσης κινδύνων και ασφάλειας των πληροφοριακών συστημάτων·

γ) οργάνωση της κυβερνοασφάλειας, συμπεριλαμβανομένου του καθορισμού ρόλων και αρμοδιοτήτων·

δ) διαχείριση περιουσιακών στοιχείων, συμπεριλαμβανομένης της απογραφής περιουσιακών στοιχείων ΤΠ και της χαρτογράφησης του δικτύου ΤΠ·

ε) ασφάλεια των ανθρώπινων πόρων και έλεγχος πρόσβασης·

στ) ασφάλεια των επιχειρήσεων·

ζ) ασφάλεια των επικοινωνιών·

η) απόκτηση, ανάπτυξη και συντήρηση συστημάτων, συμπεριλαμβανομένου του χειρισμού και της γνωστοποίησης τρωτοτήτων·

θ) ασφάλεια της αλυσίδας εφοδιασμού, συμπεριλαμβανομένων των πτυχών που αφορούν την ασφάλεια ως προς τις σχέσεις μεταξύ κάθε οντότητας της Ένωσης και των άμεσων προμηθευτών ή παρόχων υπηρεσιών της. Οι οντότητες της Ένωσης λαμβάνουν υπόψη τις ιδιαίτερες τρωτότητες κάθε άμεσου προμηθευτή και παρόχου υπηρεσιών, καθώς και τη συνολική ποιότητα των προϊόντων και τις πρακτικές κυβερνοασφάλειας των προμηθευτών και των παρόχων υπηρεσιών τους, συμπεριλαμβανομένων των διαδικασιών ασφαλούς ανάπτυξής τους·

ι) χειρισμός περιστατικών και συνεργασία με τη CERT-EE, όπως η διατήρηση της παρακολούθησης της ασφάλειας και της καταγραφής·

ια) διαχείριση της επιχειρησιακής συνέχειας, όπως διαχείριση εφεδρειών και αποκατάσταση της λειτουργίας έπειτα από καταστροφή, και διαχείριση κρίσεων· και

ιβ) προώθηση και ανάπτυξη προγραμμάτων εκπαίδευσης, απόκτησης δεξιοτήτων, ευαισθητοποίησης, πρακτικής εξάσκησης και κατάρτισης στον τομέα της κυβερνοασφάλειας.

4. Οι οντότητες της Ένωσης εξετάζουν τουλάχιστον τα ακόλουθα ειδικά μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας κατά την εφαρμογή των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας στο πλαίσιο των σχεδίων κυβερνοασφάλειάς τους, σύμφωνα με τα έγγραφα καθοδήγησης και τις συστάσεις του ΠΣΒ:

α) στόχους και προτεραιότητες όσον αφορά τη χρήση υπηρεσιών νεφοϋπολογιστικής κατά την έννοια του άρθρου 4 παράγραφος 19 της οδηγίας [πρόταση οδηγίας NIS 2] και τις τεχνικές ρυθμίσεις που καθιστούν δυνατή την τηλεργασία·

β) συγκεκριμένα μέτρα για τη μελλοντική χρήση των αρχών μηδενικής εμπιστοσύνης, περιλαμβανομένου ενός μοντέλου ασφάλειας, και μια συντονισμένη στρατηγική κυβερνοασφάλειας και διαχείρισης συστήματος με βάση την αναγνώριση της ύπαρξης απειλών τόσο εντός όσο και εκτός των παραδοσιακών ορίων του δικτύου·

γ) εφαρμογή, κατά κανόνα, της πολυπαραγοντικής επαλήθευσης ταυτότητας σε όλα τα δικτυακά και πληροφοριακά συστήματα·

δ) επίτευξη ασφάλειας στην αλυσίδα εφοδιασμού λογισμικού μέσω κριτηρίων για την ασφαλή ανάπτυξη και αξιολόγηση λογισμικού·

ε) ενίσχυση των κανόνων για τη σύναψη συμβάσεων, ώστε να διευκολυνθεί η επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας μέσω:

i) της άρσης των συμβατικών φραγμών που περιορίζουν την κοινοποίηση από τους παρόχους υπηρεσιών ΤΠ στη CERT-ΕΕ πληροφοριών σχετικά με περιστατικά, τρωτότητες και κυβερνοαπειλές·

ii) της συμβατικής υποχρέωσης αναφοράς περιστατικών, τρωτοτήτων και κυβερνοαπειλών, καθώς και εφαρμογής κατάλληλης αντιμετώπισης και παρακολούθησης περιστατικών·

στ) της χρήσης κρυπτογράφησης και κρυπτοθέτησης, και ιδίως της διατερματικής κρυπτογράφησης·

ζ) ασφαλών συστημάτων επικοινωνίας εντός του οργανισμού.

Άρθρο 6

Αξιολογήσεις του επιπέδου ωριμότητας

1. Κάθε […] **οντότητα** της Ένωσης**, κατά περίπτωση με τη συνδρομή ειδικευμένου τρίτου μέρους,** διενεργεί αξιολόγηση του επιπέδου ωριμότητας […] τουλάχιστον ανά τριετία, ενσωματώνοντας όλα τα στοιχεία του οικείου περιβάλλοντος ΤΠ, όπως περιγράφεται στο άρθρο 4, λαμβάνοντας υπόψη τα σχετικά έγγραφα καθοδήγησης και τις συστάσεις που εκδίδονται σύμφωνα με το άρθρο 13.

2. Το ΙΙCB, κατόπιν σύστασης της CERT-EE και κατόπιν διαβούλευσης με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), εκδίδει, εντός 4 μηνών από την έναρξη ισχύος του παρόντος κανονισμού, μεθοδολογικές κατευθυντήριες γραμμές για τη διενέργεια αξιολογήσεων του επιπέδου ωριμότητας.

3. **Αφού ολοκληρωθεί η αξιολόγηση του επιπέδου ωριμότητας** […]**, η οντότητα της Ένωσης την υποβάλλει στο ΙΙCB. Η πρώτη αξιολόγηση του επιπέδου ωριμότητας διενεργείται το αργότερο [12 μήνες μετά την έναρξη ισχύος του παρόντος κανονισμού].**

Άρθρο 7

Σχέδια κυβερνοασφάλειας

1. Σε συνέχεια των συμπερασμάτων που προκύπτουν από την αξιολόγηση του επιπέδου ωριμότητας και λαμβανομένων υπόψη των περιουσιακών στοιχείων και των κινδύνων που εντοπίζονται σύμφωνα με το άρθρο 4, το ανώτατο διοικητικό επίπεδο κάθε [...] **οντότητας** της Ένωσης εγκρίνει σχέδιο κυβερνοασφάλειας χωρίς αδικαιολόγητη καθυστέρηση έπειτα από τη θέσπιση του πλαισίου [...]**l**, [...] **την υιοθέτηση των** [...] **μέτρων διαχείρισης κινδύνων** κυβερνοασφάλειας [...]**, καθώς και τη διεξαγωγή της αξιολόγησης του επιπέδου ωριμότητας, το αργότερο εντός 21 μηνών από την έναρξη ισχύος του παρόντος κανονισμού**. Το σχέδιο **κυβερνοασφάλειας** αποσκοπεί στην αύξηση της συνολικής κυβερνοασφάλειας της [...] **οικείας** οντότητας **της Ένωσης** και, ως εκ τούτου, συμβάλλει στην [...] ενίσχυση υψηλού κοινού επιπέδου κυβερνοασφάλειας μεταξύ όλων των [...] **οντοτήτων** της Ένωσης. [...] **Το** σχέδιο **κυβερνοασφάλειας** περιλαμβάνει τουλάχιστον τα **μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας σύμφωνα με το άρθρο 5** [...]. Το σχέδιο **κυβερνοασφάλειας** αναθεωρείται τουλάχιστον ανά **διετία** [...] **ή** έπειτα από [...] **κάθε** αξιολόγηση του επιπέδου ωριμότητας που διενεργείται σύμφωνα με το άρθρο 6 **ή κάθε αναθεώρηση του πλαισίου σύμφωνα με το άρθρο 4.**

2. [...]

3. Το σχέδιο κυβερνοασφάλειας **λαμβάνει υπόψη** [...] τυχόν εφαρμοστέα έγγραφα καθοδήγησης και συστάσεις που εκδίδονται **σύμφωνα με το άρθρο 13** [...].

4. **Αφού ολοκληρωθεί το σχέδιο κυβερνοασφάλειας, η οντότητα της Ένωσης την υποβάλλει στο ΙΙΣΒ**.

Άρθρο 7α

Αξιολόγηση από ομοτίμους

1. Το ΠΣΒ, κατόπιν σύστασης της CERT-ΕΕ και διαβούλευσης με τον ENISA, το αργότερο έως ... [24 μήνες έπειτα από την έναρξη ισχύος του παρόντος κανονισμού], χρησιμοποιώντας τη μεθοδολογία της αξιολόγησης από ομοτίμους και τη μεθοδολογία αυτοαξιολόγησης σύμφωνα με το άρθρο 16 της οδηγίας [πρόταση οδηγίας NIS 2] προσαρμοσμένων κατά περίπτωση στις ανάγκες των οντοτήτων της Ένωσης, καθορίζει τη μεθοδολογία και τις οργανωσιακές πτυχές των αξιολογήσεων από ομοτίμους με στόχο την άντληση πληροφοριών από κοινές εμπειρίες, την ενδυνάμωση της αμοιβαίας εμπιστοσύνης, την εξασφάλιση υψηλού επιπέδου κυβερνοασφάλειας, καθώς και την ενίσχυση των ικανοτήτων κυβερνοασφάλειας των οντοτήτων της Ένωσης και των σχετικών πολιτικών που απαιτούνται για την υλοποίηση του παρόντος κανονισμού. Η συμμετοχή στην αξιολόγηση από ομοτίμους είναι προαιρετική. Εκπρόσωποι των κρατών μελών μπορούν να συμμετέχουν ως παρατηρητές στην αξιολόγηση από ομοτίμους. Οι αξιολογήσεις από ομοτίμους διενεργούνται από εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας που έχουν οριστεί από τουλάχιστον δύο οντότητες της Ένωσης, διαφορετικές από τις αξιολογούμενες οντότητες της Ένωσης, και καλύπτουν τουλάχιστον ένα από τα ακόλουθα σημεία:

(i) το επίπεδο εφαρμογής των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας και των υποχρεώσεων αναφοράς περιστατικών που αναφέρονται στα άρθρα 5 και 20·

(ii) το επίπεδο ικανοτήτων, συμπεριλαμβανομένων των διαθέσιμων οικονομικών, τεχνικών και ανθρώπινων

πόρων·

(iii) το επίπεδο εφαρμογής του πλαισίου ανταλλαγής πληροφοριών, που αναφέρεται στο άρθρο 19·

(iv) ειδικά ζητήματα διατομεακού χαρακτήρα.

2. Οι οντότητες της Ένωσης μπορούν να επισημαίνουν συγκεκριμένα ζητήματα που αναφέρονται στην παράγραφο 1 σημείο iv) για να υποβληθούν σε αξιολόγηση. Το πεδίο εφαρμογής της αξιολόγησης, συμπεριλαμβανομένων των ζητημάτων που έχουν επισημανθεί, κοινοποιείται στις συμμετέχουσες οντότητες της Ένωσης πριν από την έναρξη της αξιολόγησης από ομοτίμους.

3. Πριν από την έναρξη της αξιολόγησης από ομοτίμους, οι οντότητες της Ένωσης μπορούν να διενεργούν αυτοαξιολόγηση των αξιολογούμενων πτυχών την οποία παρέχουν στους ορισθέντες εμπειρογνώμονες.

4. Στο πλαίσιο των αξιολογήσεων από ομοτίμους πραγματοποιούνται επιτόπιες επισκέψεις σε φυσικό χώρο ή μέσω διαδικτύου και ανταλλαγές εκτός των εγκαταστάσεων. Με βάση την αρχή της καλής συνεργασίας, οι οντότητες της Ένωσης που υπόκεινται σε αξιολόγηση από ομοτίμους παρέχουν στους ορισθέντες εμπειρογνώμονες τις πληροφορίες που είναι αναγκαίες για την αξιολόγηση, με την επιφύλαξη της εθνικής ή ενωσιακής νομοθεσίας σχετικά με την προστασία ευαίσθητων ή διαβαθμισμένων πληροφοριών. Κάθε πληροφορία που λαμβάνεται μέσω της διαδικασίας αξιολόγησης από ομοτίμους χρησιμοποιείται αποκλειστικά για τον σκοπό αυτό. Οι εμπειρογνώμονες που συμμετέχουν στην αξιολόγηση από ομοτίμους δεν αποκαλύπτουν σε τρίτους τυχόν ευαίσθητες ή διαβαθμισμένες πληροφορίες που απέκτησαν κατά τη διάρκεια της εν λόγω αξιολόγησης.

5. Αφού υποβληθούν σε αξιολόγηση από ομοτίμους, οι πτυχές που αξιολογήθηκαν σε οντότητες της Ένωσης δεν υπόκεινται σε περαιτέρω αξιολόγηση από ομοτίμους στις ίδιες οντότητες της Ένωσης για τα δύο έτη που ακολουθούν την ολοκλήρωση της αξιολόγησης από ομοτίμους, εκτός εάν οι οντότητες της Ένωσης το ζητήσουν ή εάν συμφωνηθεί μετά από πρόταση του ΠΣΒ.

6. Πριν από την έναρξη της αξιολόγησης από ομοτίμους, οι οντότητες της Ένωσης διασφαλίζουν ότι οι άλλες οντότητες της Ένωσης και το ΠΣΒ λαμβάνουν γνώση τυχόν κινδύνου σύγκρουσης συμφερόντων όσον αφορά τους ορισθέντες εμπειρογνώμονες. Οι οντότητες της Ένωσης που υπόκεινται σε αξιολόγηση από ομοτίμους μπορούν να αντιταχθούν στον διορισμό συγκεκριμένων εμπειρογνωμόνων για δεόντως αιτιολογημένους λόγους οι οποίοι κοινοποιούνται στις οντότητες της Ένωσης που τους ορίζουν.

7. Οι εμπειρογνώμονες που συμμετέχουν σε αξιολογήσεις από ομοτίμους συντάσσουν εκθέσεις σχετικά με τα ευρήματα και τα συμπεράσματα των αξιολογήσεων. Οι οντότητες της Ένωσης έχουν τη δυνατότητα να υποβάλουν παρατηρήσεις σχετικά με τα αντίστοιχα σχέδια εκθέσεών τους, οι οποίες επισυνάπτονται στις εκθέσεις. Οι εκθέσεις περιλαμβάνουν συστάσεις για τη βελτίωση των πτυχών που καλύπτει η αξιολόγηση από ομοτίμους. Οι εκθέσεις υποβάλλονται στο IICB και στο δίκτυο CSIRT, κατά περίπτωση. Οι αξιολογούμενες οντότητες της Ένωσης μπορούν να αποφασίσουν να δημοσιοποιήσουν την έκθεσή τους ή αναδιατυπωμένη έκδοση της έκθεσής τους.

Άρθρο 8

Εφαρμογή

1. [...]

2. Τα έγγραφα καθοδήγησης και οι συστάσεις, που εκδίδονται σύμφωνα με το άρθρο 13, υποστηρίζουν την εφαρμογή των διατάξεων του παρόντος κεφαλαίου.

3. Κατόπιν αιτήματος του IICB, οι οντότητες της Ένωσης υποβάλλουν εκθέσεις σχετικά με συγκεκριμένες πτυχές του παρόντος κεφαλαίου.

Κεφάλαιο III
ΔΙΟΡΓΑΝΙΚΟ ΣΥΜΒΟΥΛΙΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Άρθρο 9

Διοργανικό συμβούλιο κυβερνοασφάλειας

1. Ιδρύεται διοργανικό συμβούλιο κυβερνοασφάλειας (στο εξής: IICB).

2. Το IICB είναι αρμόδιο για:

   α) την παρακολούθηση της εφαρμογής του παρόντος κανονισμού από τις **οντότητες** [...] **της Ένωσης**·

   β) την εποπτεία της υλοποίησης των γενικών προτεραιοτήτων και στόχων από τη CERT-ΕΕ και την παροχή στρατηγικών κατευθύνσεων στη CERT-ΕΕ.

3. Το IICB αποτελείται από**:**

   α) έναν εκπρόσωπο που ορίζει καθένας από τους ακόλουθους φορείς:

      i) το Ευρωπαϊκό Κοινοβούλιο·

      ii) το Ευρωπαϊκό Συμβούλιο·

      iii) το Συμβούλιο της Ευρωπαϊκής Ένωσης·

      iv) η Ευρωπαϊκή Επιτροπή·

      v) το Δικαστήριο της Ευρωπαϊκής Ένωσης·

      vi) η Ευρωπαϊκή Κεντρική Τράπεζα·

vii) το Ευρωπαϊκό Ελεγκτικό Συνέδριο·

viii) η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης·

ix) η Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή·

x) η Ευρωπαϊκή Επιτροπή των Περιφερειών·

xi) η Ευρωπαϊκή Τράπεζα Επενδύσεων·

xii) το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας· και

xiii) ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια·

β) τρεις εκπροσώπους [...] **τους οποίους διορίζει** το Δίκτυο Οργανισμών της Ένωσης (στο εξής: EUAN) κατόπιν πρότασης της συμβουλευτικής επιτροπής ΤΠΕ (ICTAC) του εν λόγω Δικτύου για να εκπροσωπούν τα συμφέροντα των λοιπών οργάνων και οργανισμών που διαχειρίζονται το δικό τους περιβάλλον ΤΠ. [...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

3α. Τα μέλη μπορούν να επικουρούνται από αναπληρωτή. Ο/Η πρόεδρος μπορεί να προσκαλέσει και άλλους εκπροσώπους των **οντοτήτων** [...] που απαριθμούνται ανωτέρω ή άλλων [...] **οντοτήτων** της Ένωσης να παραστούν στις συνεδριάσεις του ΙΙCB χωρίς δικαίωμα ψήφου.

4. Το ΙΙCB θεσπίζει τον εσωτερικό κανονισμό του.

5. Το ΙΙCB ορίζει πρόεδρο, σύμφωνα με τον εσωτερικό κανονισμό του, μεταξύ των μελών του για [...] **διετή** θητεία. Το πρόσωπο που τον/την αναπληρώνει καθίσταται τακτικό μέλος του ΙΙCB για την ίδια θητεία.

6. Το ΙΙCB συνεδριάζει **τουλάχιστον τρεις φορές ανά έτος** με πρωτοβουλία του/της προέδρου του **και/ή** κατόπιν αιτήματος της CERT-ΕΕ **και/**ή κατόπιν αιτήματος οποιουδήποτε από τα μέλη του.

7. Κάθε μέλος του ΙΙCB διαθέτει μία ψήφο. Οι αποφάσεις του ΙΙCB λαμβάνονται με απλή πλειοψηφία, εκτός εάν προβλέπεται διαφορετικά στον παρόντα κανονισμό. Ο/Η πρόεδρος δεν ψηφίζει παρά μόνο σε περίπτωση ισοψηφίας, οπότε υπερισχύει η δική του/της ψήφος.

8. Το ΙΙCB μπορεί να ενεργεί με απλουστευμένη γραπτή διαδικασία που κινείται σύμφωνα με τον εσωτερικό κανονισμό του ΙΙCB. Σύμφωνα με τη διαδικασία αυτή, η σχετική απόφαση θεωρείται εγκριθείσα εντός της προθεσμίας που ορίζει ο/η πρόεδρος, εκτός εάν ένα μέλος διατυπώσει αντιρρήσεις.

9. Ο/Η επικεφαλής της CERT-ΕΕ**, ο/η επικεφαλής της ομάδας συνεργασίας NIS**, **ο/η επικεφαλής του δικτύου EU-CyCLONe και ο/η επικεφαλής του δικτύου CSIRT** ή [...] οι αναπληρωτές **τους**, [...] **μπορούν** να συμμετέχουν **ως παρατηρητές** στις συνεδριάσεις του ΙΙCB, εκτός αν το ΙΙCB αποφασίσει διαφορετικά.

10. **Ο ENISA** [...] παρέχει γραμματειακή υποστήριξη στο ΙΙCB **και είναι υπόλογος στον/στην πρόεδρο του ΙΙCB**.

11. Οι εκπρόσωποι που ορίζονται από το EUAN κατόπιν πρότασης της συμβουλευτικής επιτροπής ΤΠΕ διαβιβάζουν τις αποφάσεις του ΙΙCB **στα μέλη του EUAN** […]. Κάθε οργανισμός ή λοιπό όργανο της Ένωσης έχει το δικαίωμα να επιστήσει την προσοχή των εκπροσώπων ή του/της προέδρου του ΙΙCB σε οποιοδήποτε ζήτημα θεωρεί ότι πρέπει να τεθεί υπόψη του ΙΙCB.

12. [...]

13. Το ΙΙCB μπορεί να **συγκροτήσει** [...] εκτελεστική επιτροπή για να το επικουρεί στο έργο του και να της αναθέσει ορισμένα από τα καθήκοντα και τις αρμοδιότητές του**, ιδίως αυτά που περιέχονται στο άρθρο 10 σημεία γ) και ε)**. Το ΙΙCB θεσπίζει τον κανονισμό της εκτελεστικής επιτροπής, συμπεριλαμβανομένων των καθηκόντων και εξουσιών της και της θητείας των μελών της.

14. Το ΙΙCB υποβάλλει έκθεση στο Συμβούλιο κάθε 12 μήνες, στην οποία περιγράφεται λεπτομερώς η πρόοδος που έχει σημειωθεί όσον αφορά την εφαρμογή του παρόντος κανονισμού και προσδιορίζεται ιδίως ο βαθμός συνεργασίας της CERT-EE με τους εθνικούς ομολόγους της σε κάθε κράτος μέλος. Η εν λόγω έκθεση παρέχει στοιχεία για την ανά διετία έκθεση σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση κατά το εν λόγω χρονικό διάστημα, σύμφωνα με το άρθρο 15 της οδηγίας [πρόταση οδηγίας NIS 2].

Άρθρο 10

Καθήκοντα του ΙΙCB

Κατά την άσκηση των αρμοδιοτήτων του, το ΙΙCB ειδικότερα:

α) [...] **παρακολουθεί και επιβλέπει αποτελεσματικά την εφαρμογή** του παρόντος κανονισμού [...] **και στηρίζει** [...] **τις οντότητες** της Ένωσης **για να ενισχύσουν την κυβερνοασφάλειά τους· για τον σκοπό αυτό, το ΙΙCB μπορεί να ζητήσει ad hoc εκθέσεις από την CERT-EE και από οντότητες της Ένωσης·**

αα) **κατόπιν στρατηγικής συζήτησης, εγκρίνει πολυετή στρατηγική για την αύξηση του επιπέδου κυβερνοασφάλειας στις οντότητες της Ένωσης, την οποία αξιολογεί τακτικά και τουλάχιστον ανά πενταετία και, κατά περίπτωση, την τροποποιεί·**

β) εγκρίνει, βάσει πρότασης **την οποία υποβάλλει ο/η** [...] επικεφαλής της CERT-ΕΕ, το ετήσιο πρόγραμμα εργασιών της CERT-ΕΕ και παρακολουθεί την εφαρμογή του·

γ) εγκρίνει, βάσει πρότασης του/της επικεφαλής της CERT-ΕΕ, τον κατάλογο υπηρεσιών της CERT-ΕΕ **και τυχόν μεταγενέστερες επικαιροποιήσεις του**·

δ) εγκρίνει, βάσει πρότασης που υποβάλλει ο/ή επικεφαλής της CERT-ΕΕ, τον ετήσιο οικονομικό προγραμματισμό των εσόδων και των εξόδων, συμπεριλαμβανομένης της στελέχωσης, για τις δραστηριότητες της CERT-ΕΕ·

ε) εγκρίνει, βάσει πρότασης του/της επικεφαλής της CERT-ΕΕ, τις λεπτομέρειες για τις συμφωνίες σε επίπεδο υπηρεσιών·

στ) εξετάζει και εγκρίνει την ετήσια έκθεση που καταρτίζει ο/η επικεφαλής της CERT-ΕΕ, η οποία καλύπτει τις δραστηριότητες της CERT-ΕΕ και την από μέρους της διαχείριση κονδυλίων·

ζ) εγκρίνει και παρακολουθεί τους βασικούς δείκτες επιδόσεων της CERT-ΕΕ, οι οποίοι καθορίζονται βάσει πρότασης του/της επικεφαλής της CERT-ΕΕ·

η) εγκρίνει ρυθμίσεις συνεργασίας, **συμφωνίες** [...] ή συμβάσεις σε επίπεδο υπηρεσιών μεταξύ της CERT-ΕΕ και άλλων οντοτήτων σύμφωνα με το άρθρο 17·

θ) συγκροτεί [...] τεχνικές συμβουλευτικές ομάδες [...] για να συνδράμουν το IICB στο έργο του, εγκρίνει την εντολή τους και ορίζει τον/την πρόεδρο κάθε ομάδας·

ι) **εγκρίνει έγγραφα καθοδήγησης και συστάσεις βάσει πρότασης της CERT-ΕΕ σύμφωνα με το άρθρο 13 και αναθέτει στη CERT-ΕΕ να εκδώσει, να αποσύρει ή να τροποποιήσει πρόταση για έγγραφα καθοδήγησης ή συστάσεις, ή πρόσκληση για ανάληψη δράσης·**

ια) λαμβάνει και αξιολογεί έγγραφα και εκθέσεις που υποβάλλουν οι οντότητες της Ένωσης δυνάμει του παρόντος κανονισμού·

ιβ) υποστηρίζει τη σύσταση άτυπης ομάδας στο πλαίσιο της οποίας συνέρχονται οι τοπικοί υπεύθυνοι κυβερνοασφάλειας όλων των οντοτήτων και, ως εκ τούτου, διευκολύνει την ανταλλαγή βέλτιστων πρακτικών και πληροφοριών σε σχέση με την εφαρμογή του παρόντος κανονισμού·

ιγ) αναπτύσσει σχέδιο διαχείρισης κρίσεων στον κυβερνοχώρο για τη στήριξη της συντονισμένης διαχείρισης σημαντικών περιστατικών σε επιχειρησιακό επίπεδο που επηρεάζουν οντότητες της Ένωσης και για τη συμβολή στην τακτική ανταλλαγή σχετικών πληροφοριών, ιδίως όσον αφορά τις επιπτώσεις και τη σοβαρότητα των σημαντικών περιστατικών και τους πιθανούς τρόπους μετριασμού.

Άρθρο 11

Συμμόρφωση

1. Το IICB**, σύμφωνα με το άρθρο 9 παράγραφος 2 και το άρθρο 10,** παρακολουθεί **αποτελεσματικά** την εφαρμογή του παρόντος κανονισμού και των εκδοθέντων εγγράφων καθοδήγησης, συστάσεων και εκκλήσεων για ανάληψη δράσης από [...] **τις οντότητες** της Ένωσης. **Για τον σκοπό αυτό, το IICB μπορεί να ζητήσει τις πληροφορίες ή την τεκμηρίωση που είναι αναγκαίες για την αξιολόγηση της ορθής εφαρμογής των διατάξεων του κανονισμού από τις οντότητες της Ένωσης. Για τους σκοπούς της θέσπισης μέτρων συμμόρφωσης δυνάμει του παρόντος άρθρου, η οικεία οντότητα της Ένωσης δεν έχει δικαίωμα ψήφου.**

2. Όταν το IICB διαπιστώσει ότι **οντότητες** [...] της Ένωσης δεν έχουν εφαρμόσει ή υλοποιήσει με αποτελεσματικό τρόπο τον παρόντα κανονισμό ή έγγραφα καθοδήγησης, συστάσεις και εκκλήσεις για ανάληψη δράσης που έχουν εκδοθεί δυνάμει του παρόντος κανονισμού, με την επιφύλαξη των εσωτερικών διαδικασιών της οικείας **[...] οντότητας** της Ένωσης **και αφού δοθεί η ευκαιρία στην οικεία οντότητα ή το ενδιαφερόμενο πρόσωπο να εκφράσουν τις απόψεις τους**, δύναται:

α) να εκδώσει προειδοποίηση **για την αντιμετώπιση, εντός συγκεκριμένου χρονικού πλαισίου, ελλείψεων που εντοπίστηκαν, συμπεριλαμβανομένων συστάσεων για την τροποποίηση εγγράφων που αφορούν την κυβερνοασφάλεια και εκδίδονται από τις οντότητες της Ένωσης βάσει του παρόντος κανονισμού**· όταν είναι αναγκαίο λόγω επιτακτικού κινδύνου κυβερνοασφάλειας, οι αποδέκτες της προειδοποίησης περιορίζονται καταλλήλως·

αα) να εκδώσει αιτιολογημένη κοινοποίηση προς οντότητα της Ένωσης, σε περίπτωση που οι ελλείψεις που επισημαίνονταν στην προειδοποίηση που είχε εκδοθεί προηγουμένως δεν αντιμετωπίστηκαν επαρκώς εντός καθορισμένου χρονοδιαγράμματος, και κοινοποιεί επισήμως την εν λόγω γνώμη στο Συμβούλιο, το Ευρωπαϊκό Κοινοβούλιο και την Επιτροπή·

β) **να εκδώσει, ειδικότερα:** [...]

i. σύσταση για τη διενέργεια ελέγχου σε οντότητα της Ένωσης·

ii. αίτημα διενέργειας ελέγχου από τρίτο φορέα παροχής υπηρεσιών ελέγχου.

γ) να ζητήσει από την οντότητα της Ένωσης να διασφαλίσει τη συμμόρφωση της διαχείρισης, της διακυβέρνησης και του ελέγχου των κινδύνων κυβερνοασφάλειας με τις διατάξεις του παρόντος κανονισμού, κατά περίπτωση, με συγκεκριμένο τρόπο και εντός καθορισμένης προθεσμίας.

δ) να απευθύνει επίσημη προειδοποίηση σε όλα τα κράτη μέλη και τις οντότητες της Ένωσης στην οποία θα συστήνει προσωρινή αναστολή των ροών δεδομένων προς την οντότητα της Ένωσης.

3. Στις περιπτώσεις που το ΙΙΣΒ έχει θεσπίσει μέτρα σύμφωνα με την παράγραφο 2 στοιχεία α) έως δ), η οικεία οντότητα της Ένωσης παρέχει λεπτομερή απολογισμό των μέτρων και των δράσεων που έχουν αναληφθεί για την αντιμετώπιση των εικαζόμενων ελλείψεων που εντόπισε το ΙΙΣΒ. Η οντότητα της Ένωσης υποβάλλει τον απολογισμό εντός εύλογου χρονικού διαστήματος που συμφωνείται με το ΙΙΣΒ.

4. Όταν το ΙΙΣΒ θεωρεί ότι υπάρχει συνεχής παραβίαση των διατάξεων του παρόντος κανονισμού από οντότητα της Ένωσης ως άμεση απόρροια ενεργειών ή παραλείψεων υπαλλήλου ή μέλους του λοιπού προσωπικού της Ένωσης, συμπεριλαμβανομένων προσώπων στο ανώτατο διοικητικό επίπεδο, το ΙΙΣΒ ζητεί από την οικεία οντότητα να λάβει τα κατάλληλα μέτρα, μεταξύ άλλων μέτρα πειθαρχικού χαρακτήρα, σύμφωνα, ιδίως, με τους κανόνες που ορίζονται στον κανονισμό υπηρεσιακής κατάστασης και το καθεστώς που εφαρμόζεται στο λοιπό προσωπικό της Ευρωπαϊκής Ένωσης. Για τον σκοπό αυτό, το ΙΙΣΒ διαβιβάζει τις απαραίτητες πληροφορίες στην οικεία οντότητα.

Κεφάλαιο IV
CERT-ΕΕ

Άρθρο 12

Αποστολή και καθήκοντα της CERT-ΕΕ

1. [...] [...] **Αποστολή της CERT-ΕΕ** είναι να συμβάλλει στην ασφάλεια του μη διαβαθμισμένου περιβάλλοντος ΤΠ όλων των [...] **οντοτήτων** της Ένωσης παρέχοντας σε αυτές συμβουλές σχετικά με την κυβερνοασφάλεια, βοηθώντας τις στην πρόληψη, στον εντοπισμό, στον μετριασμό και στην αντιμετώπιση περιστατικών και λειτουργώντας για αυτές ως κόμβος συντονισμού για την ανταλλαγή πληροφοριών και την αντιμετώπιση περιστατικών στον τομέα της κυβερνοασφάλειας.

1α. Η CERT-ΕΕ συγκεντρώνει, διαχειρίζεται, αναλύει και ανταλλάσσει πληροφορίες με τις οντότητες της Ένωσης σχετικά με απειλές, τρωτότητες και περιστατικά σε μη διαβαθμισμένες υποδομές ΤΠΕ. Συντονίζει την αντιμετώπιση περιστατικών σε διοργανικό επίπεδο και σε επίπεδο οντοτήτων της Ένωσης, μεταξύ άλλων παρέχοντας εξειδικευμένη επιχειρησιακή βοήθεια ή συντονίζοντας την παροχή της.

2. Η CERT-ΕΕ εκτελεί τα ακόλουθα καθήκοντα για [...] **τις οντότητες** της Ένωσης:

α) τις στηρίζει κατά την εφαρμογή του παρόντος κανονισμού και συμβάλλει στον συντονισμό της εφαρμογής του παρόντος κανονισμού μέσω των μέτρων που παρατίθενται στο άρθρο 13 παράγραφος 1 ή μέσω ad-hoc εκθέσεων τις οποίες ζητά το ΙΙCB·

β) [...] **προσφέρει συνήθεις υπηρεσίες CSIRT για όλες τις οντότητες της Ένωσης με** δέσμη υπηρεσιών κυβερνοασφάλειας που περιγράφονται στον κατάλογο υπηρεσιών της (στο εξής: βασικές υπηρεσίες)·

γ) διατηρεί δίκτυο ομοτίμων και εταίρων για τη στήριξη των υπηρεσιών που περιγράφονται στα άρθρα 16 και 17·

δ) εφιστά την προσοχή του ΙΙCB σε κάθε ζήτημα που αφορά την εφαρμογή του παρόντος κανονισμού και την εφαρμογή των εγγράφων καθοδήγησης, των συστάσεων και των εκκλήσεων για ανάληψη δράσης·

ε) **με βάση τις πληροφορίες που αναφέρονται στην παράγραφο 1α,** [...] συμβάλλει στην επίγνωση της κατάστασης στον κυβερνοχώρο στην ΕΕ **σε στενή συνεργασία με τον ENISA. Οι πληροφορίες κοινοποιούνται και στο ΙΙCB, καθώς και στο δίκτυο CSIRT και το EU-INTCEN·**

στ) ενεργεί ως το ισοδύναμο του ορισθέντος συντονιστικού φορέα για τις οντότητες της Ένωσης, όπως αναφέρεται στο άρθρο 6 της οδηγίας [πρόταση NIS 2].

[...]

[...]

[...]

[...]

[...]

4. **Στο πλαίσιο των αρμοδιοτήτων,** η CERT-ΕΕ συμμετέχει σε διαρθρωμένη συνεργασία με τον [...] **ENISA** όσον αφορά την ανάπτυξη ικανοτήτων, την επιχειρησιακή συνεργασία και τις μακροπρόθεσμες στρατηγικές αναλύσεις των κυβερνοαπειλών σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

5. Η CERT-ΕΕ μπορεί να παρέχει τις κάτωθι υπηρεσίες που δεν περιγράφονται στον κατάλογο υπηρεσιών της (στο εξής: χρεώσιμες υπηρεσίες):

   α) υπηρεσίες που υποστηρίζουν την κυβερνοασφάλεια του περιβάλλοντος ΤΠ των [...] **οντοτήτων** της Ένωσης, πέραν αυτών που αναφέρονται στην παράγραφο 2, βάσει συμφωνιών επιπέδου υπηρεσιών και υπό την προϋπόθεση ότι υπάρχουν οι διαθέσιμοι πόροι·

   β) υπηρεσίες που υποστηρίζουν δραστηριότητες ή έργα των [...] **οντοτήτων**, της Ένωσης στον τομέα της κυβερνοασφάλειας, πέραν αυτών που αποσκοπούν στην προστασία του περιβάλλοντος ΤΠ των οργάνων αυτών, βάσει γραπτών συμφωνιών και με την προηγούμενη έγκριση του ΙΙCB·

   γ) υπηρεσίες που υποστηρίζουν την ασφάλεια του περιβάλλοντος ΤΠ σε οργανισμούς άλλους πέραν των [...] **οντοτήτων** της Ένωσης που συνεργάζονται στενά με [...] **οντότητες** της Ένωσης, για παράδειγμα με την ανάθεση καθηκόντων ή αρμοδιοτήτων δυνάμει του ενωσιακού δικαίου, βάσει γραπτών συμφωνιών και με την προηγουμένη έγκριση του ΙΙCB.

6. Η CERT-ΕΕ μπορεί να διοργανώνει **ή να συμμετέχει σε** ασκήσεις κυβερνοασφάλειας ή να συστήνει τη συμμετοχή σε υφιστάμενες ασκήσεις, σε στενή συνεργασία με [...] **τον ENISA**, κατά περίπτωση, με σκοπό τη δοκιμή του επιπέδου κυβερνοασφάλειας των [...] **οντοτήτων** της Ένωσης.

7. Η CERT-ΕΕ μπορεί να παρέχει συνδρομή σε [...] **οντότητες** της Ένωσης όσον αφορά περιστατικά σε διαβαθμισμένα περιβάλλοντα ΤΠ, κατόπιν σχετικού ρητού αιτήματος από **τις οικείες οντότητες της Ένωσης**[...] **σύμφωνα με τις αντίστοιχες διαδικασίες τους.**. **Στην περίπτωση αυτή δεν εφαρμόζονται οι διατάξεις των άρθρων 19 έως 21 του παρόντος κανονισμού. Η παροχή συνδρομής από τη CERT-ΕΕ δυνάμει της παρούσας παραγράφου δεν θίγει τους ισχύοντες κανόνες των κρατών μελών ή της Ένωσης σχετικά με την προστασία ευαίσθητων ή διαβαθμισμένων πληροφοριών.**

8. Η CERT-ΕΕ ενημερώνει τις οντότητες της Ένωσης σχετικά με τις διαδικασίες και διεργασίες που ακολουθεί για τη διαχείριση περιστατικών.

9. Η CERT-ΕΕ μπορεί να παρακολουθεί την κίνηση του δικτύου των οντοτήτων της Ένωσης με τη συναίνεση της οικείας οντότητας της Ένωσης.

10. Η CERT-ΕΕ μπορεί, εφόσον ζητηθεί ρητά από τμήματα πολιτικής των οντοτήτων της Ένωσης, να συνεισφέρει τεχνικές συμβουλές ή στοιχεία για συναφή ζητήματα πολιτικής.

11. Η CERT-ΕΕ, σε συνεργασία με τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων, στηρίζει τις οικείες οντότητες της Ένωσης κατά την αντιμετώπιση περιστατικών που οδηγούν σε παραβιάσεις δεδομένων προσωπικού χαρακτήρα.

Άρθρο 13

Έγγραφα καθοδήγησης, συστάσεις και εκκλήσεις για ανάληψη δράσης

1. Η CERT-ΕΕ υποστηρίζει την εφαρμογή του παρόντος κανονισμού εκδίδοντας:

   α) εκκλήσεις για ανάληψη δράσης που περιγράφουν επείγοντα μέτρα ασφάλειας τα οποία καλούνται να λάβουν [...] οι οντότητες της Ένωσης εντός καθορισμένου χρονικού πλαισίου. Αφού λάβει την έκκληση για ανάληψη δράσης, η οικεία οντότητα της Ένωσης ενημερώνει, χωρίς αδικαιολόγητη καθυστέρηση, τη CERT-ΕΕ σχετικά με τον τρόπο εφαρμογής των εν λόγω μέτρων·

   β) προτάσεις προς το ΙΙCB για έγγραφα καθοδήγησης που απευθύνονται σε όλα ή σε υποσύνολο των [...] **οντοτήτων** της Ένωσης·

   γ) προτάσεις προς το ΙΙCB για συστάσεις που απευθύνονται σε μεμονωμένες [...] **οντότητες** της Ένωσης.

2. Τα έγγραφα καθοδήγησης και οι συστάσεις μπορούν να περιλαμβάνουν:

   α) λεπτομέρειες ή βελτιώσεις για τη διαχείριση κινδύνων κυβερνοασφάλειας και **τα μέτρα διαχείρισης κινδύνων** [...] κυβερνοασφάλειας·

   β) λεπτομέρειες για τις αξιολογήσεις του επιπέδου ωριμότητας και τα σχέδια κυβερνοασφάλειας· και

   γ) κατά περίπτωση, τη χρήση κοινής τεχνολογίας, κοινής αρχιτεκτονικής και κοινών συναφών βέλτιστων πρακτικών με στόχο την επίτευξη διαλειτουργικότητας και κοινών προτύπων**, συμπεριλαμβανομένης μιας συντονισμένης προσέγγισης της ασφάλειας της εφοδιαστικής αλυσίδας** [...]**.**

[...]

[...]

Άρθρο 14

Επικεφαλής της CERT-ΕΕ

1. Η Επιτροπή, αφού λάβει την έγκριση των δύο τρίτων των μελών του ΙΙCB, διορίζει τον/την επικεφαλής της CERT-ΕΕ. Η γνώμη του ΙΙCB ζητείται σε όλα τα στάδια της διαδικασίας που προηγείται του διορισμού του/της επικεφαλής της CERT-ΕΕ, ειδικότερα για τη σύνταξη προκηρύξεων πλήρωσης της θέσης, την εξέταση των αιτήσεων και τον ορισμό των εξεταστικών επιτροπών σε σχέση με την εν λόγω θέση.

2. Ο/Η επικεφαλής της CERT-ΕΕ είναι αρμόδιος/-α για την εύρυθμη λειτουργία της CERT-ΕΕ, ενεργώντας στο πλαίσιο των αρμοδιοτήτων της υπό την καθοδήγηση του ΙΙCB. Ο/Η επικεφαλής είναι αρμόδιος/-α για την υλοποίηση της στρατηγικής κατεύθυνσης, της καθοδήγησης, των στόχων και των προτεραιοτήτων που θέτει το ΙΙCB και για τη χρηστή διοίκηση της CERT-ΕΕ, συμπεριλαμβανομένων των οικονομικών και ανθρώπινων πόρων της. Υποβάλλει τακτικά εκθέσεις στον/στην πρόεδρο του ΙΙCB.

3. Ο/Η επικεφαλής της CERT-ΕΕ συνδράμει τον αρμόδιο κύριο διατάκτη κατά τη σύνταξη της ετήσιας έκθεσης δραστηριοτήτων η οποία περιλαμβάνει δημοσιονομικές και διαχειριστικές πληροφορίες, μεταξύ των οποίων τα αποτελέσματα ελέγχων, και η οποία συντάσσεται βάσει του άρθρου 74 παράγραφος 9 του δημοσιονομικού κανονισμού, και υποβάλλει τακτικά εκθέσεις σε αυτόν σχετικά με την εφαρμογή των μέτρων για τα οποία του έχει ανατεθεί αρμοδιότητα.

4. Ο/Η επικεφαλής της CERT-ΕΕ καταρτίζει ετησίως οικονομικό προγραμματισμό των διοικητικών εσόδων και δαπανών για τις δραστηριότητές της, την πρόταση για το ετήσιο πρόγραμμα εργασίας, την πρόταση για τον κατάλογο υπηρεσιών της CERT-ΕΕ και την αναθεώρησή του, την πρόταση σχετικά με λεπτομέρειες για συμφωνίες σε επίπεδο υπηρεσιών και την πρόταση για βασικούς δείκτες επιδόσεων της CERT-ΕΕ που πρέπει να εγκριθούν από το ΙΙCB σύμφωνα με το άρθρο 10.

Κατά την αναθεώρηση του καταλόγου υπηρεσιών της CERT-ΕΕ, ο/η επικεφαλής της CERT-ΕΕ λαμβάνει υπόψη τους πόρους που διατίθενται στη CERT-ΕΕ.

5. Ο/Η επικεφαλής της CERT-ΕΕ [...] υποβάλλει [...] **ετήσιες** εκθέσεις στο ΙΙCB και στον/στην πρόεδρο του ΙΙCB σχετικά με τις επιδόσεις της CERT-ΕΕ, τον οικονομικό σχεδιασμό, τα έσοδα, την εκτέλεση του προϋπολογισμού, τις συμφωνίες σε επίπεδο υπηρεσιών και τις γραπτές συμφωνίες που έχουν συναφθεί, τη συνεργασία με ομολόγους και εταίρους, καθώς και σχετικά με τις αποστολές που αναλαμβάνει το προσωπικό, συμπεριλαμβανομένων των εκθέσεων που αναφέρονται στο άρθρο 10 [...]**στοιχείο α)**.

Άρθρο 15

Οικονομικά θέματα και θέματα προσωπικού

[...]

1α. Παρότι η CERT-ΕΕ έχει συσταθεί ως αυτόνομος διοργανικός πάροχος υπηρεσιών για όλες τις οντότητες της Ένωσης, ενσωματώνεται στη διοικητική δομή μιας Γενικής Διεύθυνσης της Επιτροπής, προκειμένου να επωφεληθεί από τις δομές διοικητικής, οικονομικής, διαχειριστικής και λογιστικής υποστήριξης της Επιτροπής. Η Επιτροπή ενημερώνει το ΙΙCB σχετικά με την διοικητική έδρα της CERT-ΕΕ καθώς και τυχόν αλλαγές της. Η προσέγγιση αυτή αξιολογείται σε τακτική βάση, το αργότερο πριν από τη λήξη κάθε πολυετούς δημοσιονομικού πλαισίου που θεσπίζεται σύμφωνα με το άρθρο 312 της ΣΛΕΕ, ώστε να καθίσταται δυνατή η ανάληψη ενδεδειγμένης δράσης.

2. Για την εφαρμογή των διοικητικών και δημοσιονομικών διαδικασιών, ο/η επικεφαλής της CERT-ΕΕ ενεργεί υπό τον έλεγχο της Επιτροπής.

3. Τα καθήκοντα και οι δραστηριότητες της CERT-ΕΕ, συμπεριλαμβανομένων των υπηρεσιών που παρέχονται από τη CERT-ΕΕ σύμφωνα με το άρθρο 12 παράγραφοι 2, [...] 4 και 6 και το άρθρο 13 παράγραφος 1 [...] **στις οντότητες** της Ένωσης οι οποίες χρηματοδοτούνται από τον τομέα του πολυετούς δημοσιονομικού πλαισίου που είναι αφιερωμένος στην ευρωπαϊκή δημόσια διοίκηση, χρηματοδοτούνται μέσω χωριστής γραμμής του προϋπολογισμού της Επιτροπής. Οι ειδικές θέσεις της CERT-ΕΕ περιγράφονται λεπτομερώς σε υποσημείωση του πίνακα προσωπικού της Επιτροπής.

4. [...] **Οι οντότητες** της Ένωσης, πέραν αυτών που αναφέρονται στην παράγραφο 3, καταβάλλουν ετήσια χρηματοδοτική συνεισφορά στη CERT-ΕΕ για την κάλυψη των υπηρεσιών που παρέχει η CERT-ΕΕ σύμφωνα με την εν λόγω παράγραφο 3. Οι αντίστοιχες συνεισφορές βασίζονται σε κατευθύνσεις που παρέχει το ΙΙCB και συμφωνούνται μεταξύ της κάθε οντότητας και της CERT-ΕΕ στο πλαίσιο συμφωνιών επιπέδου υπηρεσιών. Οι συνεισφορές αντιστοιχούν σε δίκαιο και αναλογικό ποσοστό του συνολικού κόστους των παρεχόμενων υπηρεσιών. Εισπράττονται από τη χωριστή γραμμή του προϋπολογισμού που αναφέρεται στην παράγραφο 3 ως έσοδα για ειδικό προορισμό, όπως προβλέπεται στο άρθρο 21 παράγραφος 3 στοιχείο γ) του κανονισμού (ΕΕ, Ευρατόμ) 2018/1046 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[12].

5. Οι δαπάνες για τα καθήκοντα που ορίζονται στο άρθρο 12 παράγραφος 5 ανακτώνται από [...] **τις οντότητες** της Ένωσης που λαμβάνουν τις υπηρεσίες της CERT-ΕΕ. Τα έσοδα εγγράφονται στις γραμμές του προϋπολογισμού που καλύπτουν τις δαπάνες.

---

12 Κανονισμός (ΕΕ, Ευρατόμ) αριθ. 2018/1046 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Ιουλίου 2018, σχετικά με τους δημοσιονομικούς κανόνες που εφαρμόζονται στον γενικό προϋπολογισμό της Ένωσης, την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1296/2013, (ΕΕ) αριθ. 1301/2013, (ΕΕ) αριθ. 1303/2013, (ΕΕ) αριθ. 1304/2013, (ΕΕ) αριθ. 1309/2013, (ΕΕ) αριθ. 1316/2013, (ΕΕ) αριθ. 223/2014, (ΕΕ) αριθ. 283/2014 και της απόφασης αριθ. 541/2014/ΕΕ και για την κατάργηση του κανονισμού (ΕΕ, Ευρατόμ) αριθ. 966/2012 (ΕΕ L 193 της 30.7.2018, σ. 1).

Άρθρο 16

Συνεργασία της CERT-ΕΕ με τους ομολόγους της από κράτη μέλη

1. Η CERT-ΕΕ**, χωρίς αδικαιολόγητη καθυστέρηση,** συνεργάζεται και ανταλλάσσει πληροφορίες με εθνικούς ομολόγους στα κράτη μέλη, **ιδίως** [...] [...] [...]**,** με ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT) **που αναφέρονται στο άρθρο 9 της οδηγίας [πρόταση οδηγίας NIS 2] και/ή, κατά περίπτωση, εθνικές αρμόδιες αρχές** και τα ενιαία σημεία επαφής που αναφέρονται στο άρθρο 8 της οδηγίας [πρόταση οδηγίας NIS 2], σχετικά με κυβερνοαπειλές, τρωτότητες και περιστατικά, καθώς και σχετικά με πιθανά αντίμετρα και όλα τα θέματα που αφορούν τη βελτίωση της προστασίας των περιβαλλόντων ΤΠ των [...] **οντοτήτων** της Ένωσης, μεταξύ άλλων μέσω του δικτύου CSIRT που αναφέρεται στο άρθρο 13 της οδηγίας [πρόταση οδηγίας NIS 2].

1α. Η CERT-ΕΕ ειδοποιεί, χωρίς καθυστέρηση, κάθε οικείο εθνικό ομόλογο κράτους μέλους που αναφέρεται στην παράγραφο 1, όταν λαμβάνει γνώση σημαντικών περιστατικών που συντελούνται στο έδαφος του εν λόγω κράτους μέλους, εκτός εάν η CERT-ΕΕ διαθέτει την πληροφορία ότι η θιγόμενη οντότητα της Ένωσης έχει ήδη αναφέρει τέτοιο περιστατικό σύμφωνα με το άρθρο 20 παράγραφος 2α.

2. Η CERT-ΕΕ, **χωρίς αδικαιολόγητη καθυστέρηση,** [...] ανταλλάσσει πληροφορίες σχετικά με συγκεκριμένα περιστατικά με τους εθνικούς ομολόγους στα κράτη μέλη προκειμένου να διευκολύνεται ο εντοπισμός παρόμοιων κυβερνοαπειλών ή περιστατικών **ή να συνεισφέρει στην ανάλυση ενός περιστατικού** χωρίς **να χρειάζεται η** συγκατάθεση της επηρεαζόμενης **οντότητας της Ένωσης** [...]. Η CERT-ΕΕ **δεν** [...] ανταλλάσσει πληροφορίες σχετικά με συγκεκριμένα περιστατικά που αποκαλύπτουν την ταυτότητα του στόχου του περιστατικού κυβερνοασφάλειας **παρά μόνο αν**[...]

α) η θιγόμενη οντότητα της Ένωσης έχει δώσει τη συγκατάθεσή της·

β) η θιγόμενη οντότητα της Ένωσης έχει ήδη γνωστοποιήσει ότι επηρεάστηκε·

γ) η θιγόμενη οντότητα της Ένωσης δεν έχει δώσει τη συγκατάθεσή της, αλλά η δημοσίευση της ταυτότητας της θιγόμενης οντότητας της Ένωσης θα αύξανε την πιθανότητα αποφυγής ή μετριασμού των περιστατικών αλλού. Τέτοιες αποφάσεις απαιτούν την έγκριση του/της επικεφαλής της CERT-ΕΕ. Η θιγόμενη οντότητα της Ένωσης ενημερώνεται πριν από τη δημοσίευση.

Άρθρο 17

Συνεργασία της CERT-ΕΕ με [...] ***<u>άλλους</u> ομολόγους***

1. Η CERT-ΕΕ μπορεί να συνεργάζεται με ομολόγους της **στην Ευρωπαϊκή Ένωση που δεν συγκαταλέγονται σε εκείνους που αναφέρονται στο άρθρο 16** [...], συμπεριλαμβανομένων ομολόγων ανά κλάδο, σχετικά με εργαλεία και μεθόδους, όπως τεχνικές, τακτικές, διαδικασίες και βέλτιστες πρακτικές, καθώς και σχετικά με κυβερνοαπειλές και τρωτότητες. Για κάθε συνεργασία με τους εν λόγω ομολόγους, [...] η CERT-ΕΕ ζητεί την προηγούμενη έγκριση του ΙΙCB **κατά περίπτωση. Η CERT-ΕΕ ενημερώνει τους αρμόδιους εθνικούς ομολόγους που αναφέρονται στο άρθρο 16 παράγραφος 1, σε κράτος μέλος στο οποίο βρίσκεται ο ομόλογος, όταν η CERT-ΕΕ καθιερώνει συνεργασία με τους εν λόγω ομολόγους.**

2. Η CERT-ΕΕ μπορεί να συνεργάζεται με άλλους εταίρους, όπως εμπορικές οντότητες, διεθνείς οργανισμούς, εθνικές οντότητες εκτός Ευρωπαϊκής Ένωσης ή μεμονωμένους εμπειρογνώμονες, για τη συλλογή πληροφοριών σχετικά με γενικές και ειδικές κυβερνοαπειλές, γενικές και ειδικές τρωτότητες, καθώς και γενικά και ειδικά πιθανά αντίμετρα. Για ευρύτερη συνεργασία με τους εταίρους αυτούς, η CERT-ΕΕ ζητεί την προηγούμενη έγκριση του ΙΙCB **κατά περίπτωση.**

3. Η CERT-ΕΕ μπορεί, **εφόσον έχει συναφθεί σύμβαση τήρησης του απορρήτου με τον αντίστοιχο εταίρο,** με τη συγκατάθεση της επηρεαζόμενης από περιστατικό **οντότητας της Ένωσης** [...], να παρέχει πληροφορίες σχετικά με το **συγκεκριμένο** περιστατικό στους εταίρους που **αναφέρονται στις παραγράφους 1 και 2 αποκλειστικά με σκοπό να συμβάλουν**[...] στην ανάλυση του περιστατικού. **Τέτοιοι διακανονισμοί ή συμβάσεις τήρησης του απορρήτου αποτελούν αντικείμενο νομικής επαλήθευσης σύμφωνα με τις σχετικές εσωτερικές διαδικασίες της Επιτροπής. Για τους διακανονισμούς ή τις συμβάσεις τήρησης του απορρήτου δεν απαιτείται εκ των προτέρων έγκριση από τον ΠΣΒ, αλλά ο πρόεδρός του πρέπει να ενημερώνεται σχετικά.**

4. **Η CERT-ΕΕ μπορεί κατ' εξαίρεση να συνάπτει συμφωνίες σε επίπεδο υπηρεσιών με άλλες οντότητες πέραν των οντοτήτων της Ένωσης, με προηγούμενη έγκριση του ΠΣΒ.**

Κεφάλαιο V
ΥΠΟΧΡΕΩΣΕΙΣ ΣΥΝΕΡΓΑΣΙΑΣ ΚΑΙ ΥΠΟΒΟΛΗΣ ΕΚΘΕΣΕΩΝ

Άρθρο 18

Χειρισμός πληροφοριών

1. Η CERT-ΕΕ και [...] **οι οντότητες** της Ένωσης τηρούν την υποχρέωση τήρησης του επαγγελματικού απορρήτου σύμφωνα με το άρθρο 339 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης ή ισοδύναμα εφαρμοστέα πλαίσια.

2. Οι διατάξεις του κανονισμού (ΕΚ) αριθ. 1049/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[13] εφαρμόζονται όσον αφορά αιτήματα πρόσβασης του κοινού σε έγγραφα που βρίσκονται στην κατοχή της CERT-ΕΕ, λαμβανομένης υπόψη της υποχρέωσης που απορρέει από τον εν λόγω κανονισμό για διαβούλευση με [...] **άλλες οντότητες της Ένωσης, και κατά περίπτωση τα κράτη μέλη,** όταν το αίτημα αφορά τα έγγραφά τους.

[...]

4. Ο χειρισμός πληροφοριών από τη CERT-ΕΕ και [...] **τις οντότητες** της Ένωσης συνάδει με τους **ισχύοντες** κανόνες [...] για την ασφάλεια των πληροφοριών[…].

[...]

Άρθρο 19

[...] ***Ανταλλαγή πληροφοριών στον τομέα της κυβερνοασφάλειας***

-1. Οι οντότητες της Ένωσης μπορούν να παρέχουν οικειοθελώς στη CERT-ΕΕ πληροφορίες σχετικά με κυβερνοαπειλές, περιστατικά, παρ' ολίγον περιστατικά και τρωτότητες που τις επηρεάζουν. Η CERT-ΕΕ εξασφαλίζει ότι διατίθενται αποτελεσματικά μέσα επικοινωνίας για τη διευκόλυνση της ανταλλαγής πληροφοριών με τις οντότητες της Ένωσης. Η CERT-ΕΕ μπορεί να δίνει προτεραιότητα στην επεξεργασία των υποχρεωτικών έναντι των εθελούσιων κοινοποιήσεων.

[13] Κανονισμός (ΕΚ) αριθ. 1049/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 30ής Μαΐου 2001, για την πρόσβαση του κοινού στα έγγραφα του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου και της Επιτροπής (ΕΕ L 145 της 31.5.2001, σ. 43).

1. Για να [...] **εκτελεί την αποστολή και τα καθήκοντά της όπως ορίζεται στο άρθρο 12**, η CERT-ΕΕ [...] μπορεί να ζητεί από [...] **τις οντότητες** της Ένωσης να της παρέχουν πληροφορίες από τις αντίστοιχες απογραφές των οικείων συστημάτων ΤΠ**, συμπεριλαμβανομένων πληροφοριών σχετικά με κυβερνοαπειλές, παρ' ολίγον περιστατικά, τρωτότητες, δεικτών έκθεσης σε κίνδυνο, ειδοποιήσεις επαγρύπνησης για την κυβερνοασφάλεια και συστάσεις σχετικά με την παραμετροποίηση εργαλείων κυβερνοασφάλειας για τον εντοπισμό περιστατικών στον κυβερνοχώρο** [...]. [...] **Η οντότητα της Ένωσης στην οποία** υποβάλλεται το αίτημα διαβιβάζει τις ζητούμενες πληροφορίες, καθώς και τυχόν μεταγενέστερες επικαιροποιήσεις τους, χωρίς αδικαιολόγητη καθυστέρηση.

2. [...] **Οι οντότητες** της Ένωσης, κατόπιν αιτήματος της CERT-ΕΕ και χωρίς αδικαιολόγητη καθυστέρηση, της παρέχουν ψηφιακές πληροφορίες που δημιουργούνται από τη χρήση ηλεκτρονικών συσκευών που εμπλέκονται στα αντίστοιχα περιστατικά τους. Η CERT-ΕΕ μπορεί να διευκρινίζει περαιτέρω ποια είναι τα απαιτούμενα από αυτή είδη των εν λόγω ψηφιακών πληροφοριών με σκοπό την επίγνωση της κατάστασης και την αντιμετώπιση περιστατικών.

3. Η CERT-ΕΕ μπορεί να ανταλλάσσει **με τις οντότητες της Ένωσης** πληροφορίες σχετικά με συγκεκριμένα περιστατικά που αποκαλύπτουν την ταυτότητα της επηρεαζόμενης από το περιστατικό [...] **οντότητας** της Ένωσης μόνο με τη συγκατάθεση της εν λόγω οντότητας. **Σε περίπτωση που δεν δοθεί συγκατάθεση, η ενδιαφερόμενη οντότητα παρέχει δεόντως αιτιολογημένους λόγους στη CERT-ΕΕ.** [...]

4. Οι υποχρεώσεις ανταλλαγής δεν επεκτείνονται στις διαβαθμισμένες πληροφορίες ΕΕ (ΔΠΕΕ) και στις πληροφορίες **των οποίων η διανομή πέραν της οντότητας της Ένωσης που είναι αποδέκτης έχει αποκλειστεί από την πηγή των πληροφοριών με εμφανή σήμανση, εκτός αν η πηγή των πληροφοριών** [...] **επιτρέπει ρητά την κοινοποίηση των πληροφοριών αυτών στη CERT-ΕΕ.** [...]

Άρθρο 20

[...] ***Υποχρεώσεις <u>υποβολής αναφοράς</u>***

-1. Ένα περιστατικό θεωρείται σημαντικό σε περίπτωση που:

α) έχει προκαλέσει ή είναι σε θέση να προκαλέσει σοβαρή επιχειρησιακή διαταραχή των λειτουργιών της οντότητας της Ένωσης ή οικονομική ζημία για την οικεία οντότητα της Ένωσης·

β) έχει επηρεάσει ή μπορεί να επηρεάσει άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία.

1. [...] **Όλες οι οντότητες** της Ένωσης **υποβάλλουν**[...] **στη CERT-ΕΕ:** [...]

[...].

(α) έγκαιρη προειδοποίηση, χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που έγινε αντιληπτό το σημαντικό περιστατικό, με την οποία, κατά περίπτωση, διευκρινίζεται αν υπάρχει υποψία ότι το σημαντικό περιστατικό προκλήθηκε από έκνομες ή κακόβουλες ενέργειες ή ότι θα μπορούσε να έχει διασυνοριακές επιπτώσεις·

(β) κοινοποίηση περιστατικού, χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 72 ωρών από τη στιγμή που έγινε αντιληπτό το σημαντικό περιστατικό, η οποία, κατά περίπτωση, επικαιροποιεί τις πληροφορίες που αναφέρονται στο στοιχείο α) και αναφέρει αρχική αξιολόγηση του σημαντικού περιστατικού, της σοβαρότητας και των επιπτώσεών του, καθώς και, εφόσον υπάρχουν, τις **ενδείξεις** της προσβολής·

(γ) ενδιάμεση έκθεση για τις σχετικές επικαιροποιήσεις της κατάστασης, κατόπιν αιτήματος της CERT-ΕΕ·

(δ) τελική έκθεση το αργότερο ένα μήνα μετά την υποβολή της κοινοποίησης σημαντικού περιστατικού βάσει του στοιχείου α), η οποία περιλαμβάνει τουλάχιστον τα ακόλουθα:

i) λεπτομερή περιγραφή του σημαντικού περιστατικού, της σοβαρότητας και των επιπτώσεών του·

ii) το είδος της απειλής ή τη βασική αιτία που πιθανολογείται ότι προκάλεσε το σημαντικό περιστατικό·

iii) εφαρμοζόμενα και εν εξελίξει μέτρα μετριασμού.

iv) κατά περίπτωση, τις διασυνοριακές επιπτώσεις του σημαντικού περιστατικού·

(ε) σε περιπτώσεις εν εξελίξει σημαντικών περιστατικών κατά τον χρόνο υποβολής της τελικής έκθεσης που αναφέρεται στο στοιχείο δ), έκθεση προόδου εκείνη τη στιγμή και τελική έκθεση εντός ενός μηνός από τον χειρισμό του περιστατικού.

[...]

(ζ) [...]

(η) [...]

(θ) [...]

(ι) [...]

2α. Όλες οι οντότητες της Ένωσης ανταλλάσσουν τις πληροφορίες που κοινοποιούνται σύμφωνα με την παράγραφο 1 εντός του ίδιου χρονοδιαγράμματος με αυτό που ισχύει για την ανταλλαγή πληροφοριών με τους σχετικούς εθνικούς ομολόγους που αναφέρεται στο άρθρο 16 παράγραφος 1, όπου είναι εγκατεστημένες οι οντότητες.

3. Η CERT-ΕΕ υποβάλλει [...] **στο ΙΙCB, το EU INTCEN και το δίκτυο CSIRT κάθε τρεις μήνες** [...] συνοπτική έκθεση που περιλαμβάνει ανωνυμοποιημένα και συγκεντρωτικά δεδομένα σχετικά με [...] κυβερνοαπειλές,[...] **τρωτότητες, σύμφωνα με το άρθρο 19, απαντήσεις των οντοτήτων της Ένωσης σε εκκλήσεις για δράση, σύμφωνα με το άρθρο 13 παράγραφος 1 στοιχείο α),** και σημαντικά περιστατικά που κοινοποιούνται σύμφωνα με την παράγραφο 1. **Η εν λόγω έκθεση παρέχει στοιχεία για την ανά διετία έκθεση σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση σύμφωνα με το άρθρο 15 της οδηγίας [πρόταση NIS 2].**

4. Το ΙΙCB, [...] **το αργότερο έως [6 μήνες από την ημερομηνία έναρξης της ισχύος του παρόντος κανονισμού],** εκδίδει έγγραφα καθοδήγησης ή συστάσεις **με τα οποία προσδιορίζει περαιτέρω** [...] τις λεπτομέρειες, **το μορφότυπο** και το περιεχόμενο της **έκθεσης** [...]. **Τα έγγραφα καθοδήγησης ή οι συστάσεις λαμβάνουν δεόντως υπόψη τις διατάξεις που εφαρμόζονται βάσει εκτελεστικών πράξεων, σύμφωνα με το άρθρο 20 παράγραφος 11 της οδηγίας [πρόταση NIS 2]** Η CERT-ΕΕ διαδίδει τις κατάλληλες τεχνικές λεπτομέρειες ώστε να διευκολύνει [...] **τις οντότητες** της Ένωσης στον προδραστικό εντοπισμό, στην αντιμετώπιση περιστατικών ή στην εφαρμογή μέτρων μετριασμού.

5. Οι υποχρεώσεις **υποβολής έκθεσης** [...] δεν επεκτείνονται στις ΔΠΕΕ και στις πληροφορίες **των οποίων η διανομή πέραν της οντότητας της Ένωσης που είναι αποδέκτης έχει αποκλειστεί από την πηγή των πληροφοριών με εμφανή σήμανση, εκτός αν η πηγή των πληροφοριών** [...] **επιτρέπει ρητά την κοινοποίηση των πληροφοριών αυτών στη CERT-ΕΕ.** [...]

Άρθρο 21

Συντονισμός της αντιμετώπισης περιστατικών και σχετική συνεργασία [...]

1. Ενεργώντας ως κόμβος συντονισμού για την ανταλλαγή πληροφοριών και την αντιμετώπιση περιστατικών στον τομέα της κυβερνοασφάλειας, η CERT-ΕΕ διευκολύνει την ανταλλαγή πληροφοριών σχετικά με κυβερνοαπειλές, τρωτότητες και περιστατικά μεταξύ:

   α) των [...] **οντοτήτων** της Ένωσης·

   β) των ομολόγων της που αναφέρονται στα άρθρα 16 και 17.

2. Η CERT-ΕΕ**,** [...] **σε στενή συνεργασία με τον ENISA όπου αρμόζει, σύμφωνα με το άρθρο 7 παράγραφος 7 στοιχείο δ) της πράξης για την κυβερνοασφάλεια[14],** διευκολύνει τον συντονισμό μεταξύ των [...] **οντοτήτων** της Ένωσης για την αντιμετώπιση περιστατικών, μεταξύ άλλων, με:

   α) συμβολή σε συνεπή εξωτερική επικοινωνία·

   [...]

   γ) βέλτιστη χρήση επιχειρησιακών πόρων·

   δ) συντονισμό με άλλους μηχανισμούς αντιμετώπισης κρίσεων σε επίπεδο Ένωσης.

3. Η CERT-ΕΕ **σε στενή συνεργασία με τον ENISA** στηρίζει [...] **τις οντότητες** της Ένωσης όσον αφορά την επίγνωση της κατάστασης σχετικά με τις κυβερνοαπειλές, τις τρωτότητες και τα περιστατικά.

---

14 Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια).

4. Το ΙΙCB εκδίδει**, έως [12 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού], με βάση σύσταση της CERT-ΕΕ,** [...] **έγγραφα ή συστάσεις** καθοδήγησης σχετικά με τον συντονισμό και τη συνεργασία αντιμετώπισης συμβάντων για σημαντικά περιστατικά. Όταν υπάρχουν υπόνοιες ότι ένα περιστατικό έχει ποινικό χαρακτήρα, η CERT-ΕΕ παρέχει συμβουλές σχετικά με τον τρόπο αναφοράς του περιστατικού στις αρχές επιβολής του νόμου.

Άρθρο 22

Διαχείριση σημαντικών περιστατικών [...]

-1. Για την υποστήριξη της συντονισμένης διαχείρισης σημαντικών περιστατικών σε επιχειρησιακό επίπεδο που επηρεάζουν οντότητες της Ένωσης και για τη συμβολή στην τακτική ανταλλαγή σχετικών πληροφοριών μεταξύ των οντοτήτων της Ένωσης και με τα κράτη μέλη, το ΙΙCB καταρτίζει σχέδιο διαχείρισης κρίσεων στον κυβερνοχώρο με βάση τις δραστηριότητες που περιγράφονται στο άρθρο 21 παράγραφος 2, σε στενή συνεργασία με τη CERT-ΕΕ και τον ENISA, και περιλαμβάνει, τουλάχιστον, τα ακόλουθα στοιχεία:

α) λεπτομέρειες για τον συντονισμό και τη ροή πληροφοριών μεταξύ των οντοτήτων της Ένωσης για τη διαχείριση σημαντικών περιστατικών σε επιχειρησιακό επίπεδο·

β) κοινές τυποποιημένες επιχειρησιακές διαδικασίες·

γ) κοινή ταξινόμηση της σοβαρότητας των σημαντικών περιστατικών και των σημείων που πυροδοτούν κρίσεις·

δ) τακτικές ασκήσεις·

ε) ασφαλείς διαύλους επικοινωνίας που πρέπει να χρησιμοποιούνται·

στ) ένα σημείο επαφής για το EU-CyCLONe, το οποίο ανταλλάσσει σχετικές πληροφορίες με το EU-CyCLONe ως στοιχεία για την κοινή αντίληψη της κατάστασης.

1. Η CERT-ΕΕ συντονίζει [...] **τις οντότητες** της Ένωσης κατά την αντιμετώπιση σημαντικών **περιστατικών**[...]. Τηρεί κατάλογο της τεχνικής εμπειρογνωσίας που απαιτείται για την αντιμετώπιση περιστατικών σε περίπτωση **σημαντικών περιστατικών** [...].

2. [...] **Οι οντότητες** της Ένωσης συμβάλλουν στην κατάρτιση του καταλόγου τεχνικής εμπειρογνωσίας παρέχοντας και επικαιροποιώντας σε ετήσια βάση κατάλογο των διαθέσιμων εμπειρογνωμόνων στο πλαίσιο των αντίστοιχων οργανισμών τους, στον οποίον αναφέρονται λεπτομερώς οι ειδικές τεχνικές δεξιότητές τους.

3. Έπειτα από συγκεκριμένο αίτημα κράτους μέλους στο οποίο βρίσκεται η θιγόμενη οντότητα της Ένωσης και με [...] την έγκριση **της επηρεαζόμενης** [...][...] **οντότητας**[...] της Ένωσης, η CERT-ΕΕ δύναται επίσης να ζητήσει από τους εμπειρογνώμονες του καταλόγου που αναφέρεται στην παράγραφο 2 να συμβάλουν στην αντιμετώπιση σοβαρού **περιστατικού** [...] **στην** [...] **εν λόγω οντότητα της Ένωσης** [...]**.**

ΚΕΦΑΛΑΙΟ VI
ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 23

Αρχική κατανομή των πιστώσεων του προϋπολογισμού

Η Επιτροπή προτείνει την ανακατανομή προσωπικού και οικονομικών πόρων από [...] **τις σχετικές οντότητες** της Ένωσης στον προϋπολογισμό της Επιτροπής. Η ανακατανομή τίθεται σε εφαρμογή ταυτόχρονα με τον πρώτο προϋπολογισμό που θα εγκριθεί μετά την έναρξη ισχύος του παρόντος κανονισμού.

Άρθρο 24

Επανεξέταση

1. Το IICB, με τη συνδρομή της CERT-EE, υποβάλλει περιοδικές εκθέσεις στην Επιτροπή σχετικά με την εφαρμογή του παρόντος κανονισμού. Το IICB μπορεί επίσης να απευθύνει συστάσεις στην Επιτροπή για **την αναθεώρηση** [...]του παρόντος κανονισμού.

2. Η Επιτροπή υποβάλλει έκθεση σχετικά με την εφαρμογή του παρόντος κανονισμού στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο το αργότερο **36** [...] μήνες μετά την έναρξη ισχύος του παρόντος κανονισμού και στη συνέχεια ανά τριετία.

3. Η Επιτροπή αξιολογεί τη λειτουργία του παρόντος κανονισμού και υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο, στην Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και στην Επιτροπή των Περιφερειών το **αργότερο** [...] πέντε έτη μετά την ημερομηνία έναρξης ισχύος του. **Η έκθεση συνοδεύεται, εφόσον είναι αναγκαίο, από νομοθετική πρόταση.**

Άρθρο 25

Έναρξη ισχύος

Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Βρυξέλλες,

Για το Ευρωπαϊκό Κοινοβούλιο	*Για το Συμβούλιο*
Η Πρόεδρος	*Ο Πρόεδρος / Η Πρόεδρος*

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

ΠΑΡΑΡΤΗΜΑ ΙΙ

[...]

[...]

[...]

[...]

[...]

[...]

[...]